6.2 RIP 协议

路由信息协议 RIP（Routing Information Protocol）是一个真正的距离矢量路由选择协议。它每隔 30 秒钟就送出自己完整的路由表到所有激活的接口。RIP 只使用跳数来决定到达远程网络的最佳方式，并且在默认时它所允许的最大跳数为 15 跳，也就是说 16 跳的距离将被认为是不可达的。

在小型网络中，RIP 会运转良好，但是对于使用慢速 WAN 连接的大型网络或者安装有大量路由器的网络来说，它的效率就很低了。即便是网络没有变化，也是每隔 30 秒发送路由表到所有激活的接口，占用网络带宽。

当路由器 A 意外故障 down 机，需要由它的邻居路由器 B 将路由器 A 所连接的网段不可到达的信息通告出去。路由器 B 如何断定某个路由失效？如果路由器 B 180 秒没有得到关于某个指定路由的任何更新，就认为这个路由失效。所以这个周期性更新是必须的。

RIP 版本 1 使用有类路由选择，即在该网络中的所有设备必须使用相同的子网掩码，这是因为 RIP 版本 1 不发送带有子网掩码信息的更新数据。RIP 版本 2 提供了被称为前缀路由选择的信息，并利用路由更新来传送子网掩码信息，这就是所谓的无类路由选择。

RIP 是典型的距离矢量路由选择协议，距离矢量路由选择算法发送完整的路由表到相邻的路由器，然后，相邻的路由器会将接收到的路由表项与自己原有的路由表进行组合，以完善路由器的路由表。

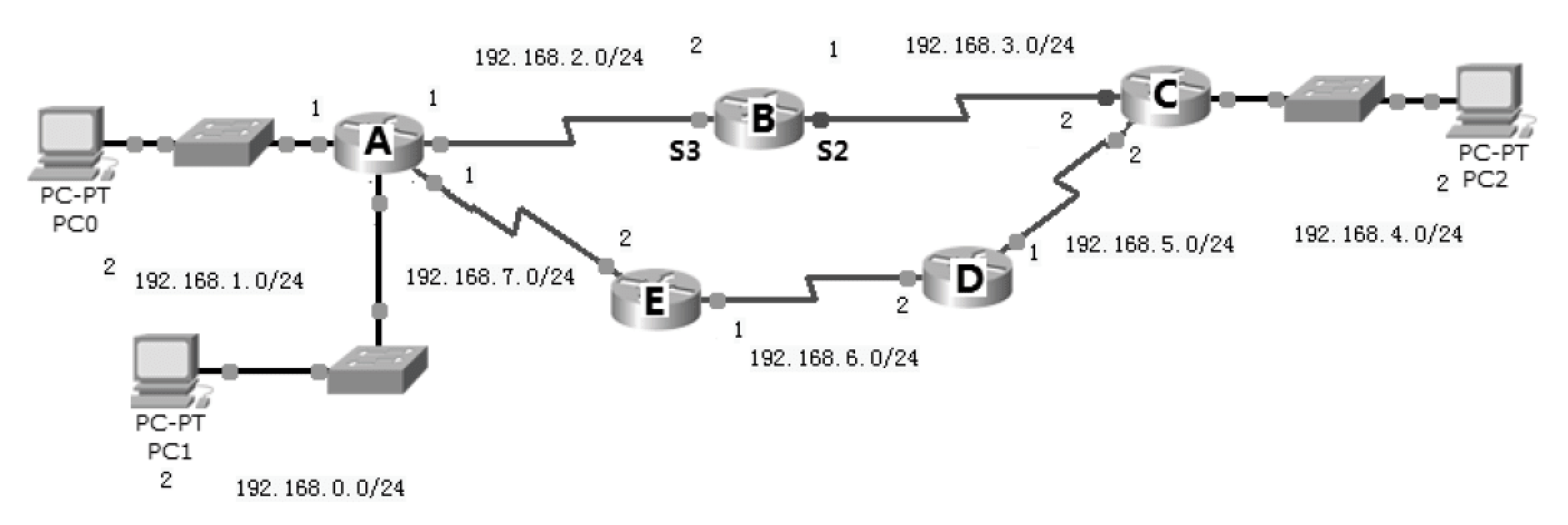
RIP 只使用跳数来决定到达某个互联网络的最佳路径。如果 RIP 发现对于同一个远程网络存在有不止一条链路，并且它们又都具有相同的跳数，则路由器将自动执行循环负载均衡。RIP 可以对多达 6 个相同开销的链路实现负载均衡（默认为 4 个）。

下面将讲解 RIP 协议的配置。

6.2.1 RIP 的配置过程

下面将会以实例演示 RIP 配置的过程，会讲解过程中使用的一些参数。

打开随书光盘中第 6 章练习“01 动态路由 RIP.pkt”，网络拓扑和 IP 地址规划如图 6-2 所示，网络中的路由器和 IP 地址已经配置好。



▲图 6-2 网络拓扑

以下步骤将会演示在 A、B、C、D 和 E 路由器上启用 RIP 协议，查看路由器上的路由表，验证配置 RIP 时，network 命令的作用，跟踪数据包从 PC0 到 PC2 的路径，验证当最佳路径不可用后，RIP 能够自动更新路由表。

操作步骤如下。

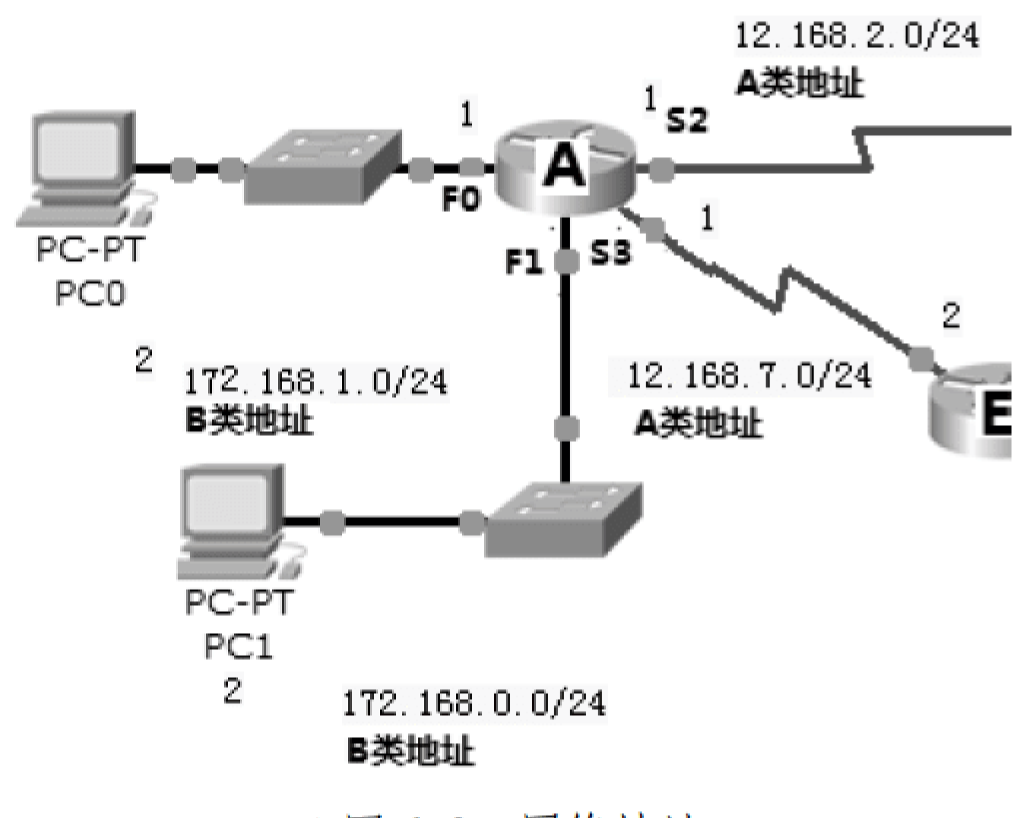
（1）在路由器 A 上，启用和配置 RIP 协议。

```
RA>en
RA#config t
RA（config）#router rip --在路由器上启用 RIP 协议
RA（config-router）#network 192.168.0.0
RA（config-router）#network 192.168.1.0
RA（config-router）#network 192.168.2.0
RA（config-router）#network 192.168.7.0
```

就这几条命令就可以了，比静态路由简单多了。

在 RA（config-router）#提示符下输入的 network 命令用于告诉此路由选择协议哪个有类网络可以进行通告。由于路由器 A 连着 4 个 C 类网络，要 network 这 4 个网络。注意，我没有输入子网，而只有有类网络地址（即所有的子网位和主机位都是 0）。这样这 4 个接口连接的网段都能够通告给其他路由器，同时这些接口也能够接收其他路由器发送过来的 RIP 信息。

思考：如图 6-3 所示，如果路由器 A 连着以下网络，network 应该怎样写呢？



▲图 6-3　网络地址

路由器 A 的 F0 和 F1 接口连接的网段属于同一个 B 类地址 172.168.0.0，路由器 A 的 S2 和 S3 接口连接的网段是同一个 A 类地址 12.0.0.0，因此需要输入以下命令让这 4 个接口参与到 RIP 的工作中。

```
RA（config）#router rip
RA（config-router）#network 172.168.0.0
RA（config-router）#network 12.0.0.0
```

下面的配置是错误的，A 类地址子网掩码默认是 255.0.0.0，子网位和主机位应归 0，network 后就不能写成 12.168.0.0。

```
RA（config-router）#network 12.168.0.0
```

（2）在路由器 B 上，启用和配置 RIP 协议。

```
RB>en
RB#config t
RB（config）#route rip
```

```
RB (config-router) #network 192.168.2.0
RB (config-router) #network 192.168.3.0
RB#show ip protocols          --显示配置的动态路由协议
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 4 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface            Send  Recv  Triggered RIP  Key-chain
  Serial3/0            1     2 1
  Serial2/0            1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
192.168.2.0                          --RIP 协议配置的 network 两个网络
192.168.3.0
Passive Interface (s) :
Routing Information Sources:
Gateway        Distance     Last Update
192.168.2.1         120     00:00:10
Distance: (default is 120)      --RIP 协议默认管理距离
```

（3）在路由器 C 上，启用和配置 RIP 协议。

```
RC (config) #router rip
RC (config-router) #net 192.168.3.0 --network 可以简写为 net
RC (config-router) #net 192.168.4.0
RC (config-router) #net 192.168.5.0
```

（4）在路由器 D 上，启用和配置 RIP 协议。

```
RD (config) #router rip
RD (config-router) #net 192.168.5.0
RD (config-router) #net 192.168.6.0
```

（5）在路由器 E 上，启用和配置 RIP 协议。

```
RE (config) #router rip
RE (config-router) #net 192.168.6.0
RE (config-router) #net 192.168.7.0
```

（6）现在网络中的路由器都已经配置了 RIP 协议，在路由器 C 上，查看路由表。

```
RC#show ip route
Gateway of last resort is not set
R    192.168.0.0/24 [120/2] via 192.168.3.1, 00:00:13, Serial2/0 --①
R    192.168.1.0/24 [120/2] via 192.168.3.1, 00:00:13, Serial2/0 --②
R    192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:13, Serial2/0 --③
C    192.168.3.0/24 is directly connected, Serial2/0            --④
C    192.168.4.0/24 is directly connected, FastEthernet0/0      --⑤
C    192.168.5.0/24 is directly connected, Serial3/0            --⑥
R    192.168.6.0/24 [120/1] via 192.168.5.1, 00:00:03, Serial3/0 --⑦
R    192.168.7.0/24 [120/2] via 192.168.3.1, 00:00:13, Serial2/0 --⑧
                  [120/2] via 192.168.5.1, 00:00:03, Serial3/0    --⑨
```

R 代表通过 RIP 协议学习到的路由。

C 代表直连的网络。

注意看第①条和第②条路由，[120/2]，120 表示管理距离，2 代表度量值，表示到达 192.168.0.0/24 和 192.168.1.0/24 网段需要经过两个路由器，via 后面的地址是下一跳转发给哪个地址。

> **注意** 看第⑧条和⑨条路由，这两条路由代表到达 192.168.7.0/24 网段有两条等价路径。

（7）在路由器 A 上，不让 192.168.0.0/24 网段参与 RIP 协议。

```
RA (config) #route rip
RA (config-router) #no network 192.168.0.0 --取消这个C类网络参与RIP协议
```

（8）在路由器 C 上，查看路由表，看看是否还有到 192.168.0.0 网段的路由。

RC#clear ip route *：该命令将会清空路由器学习到的所有路由，稍等一会儿就会重新学习到正确路由。

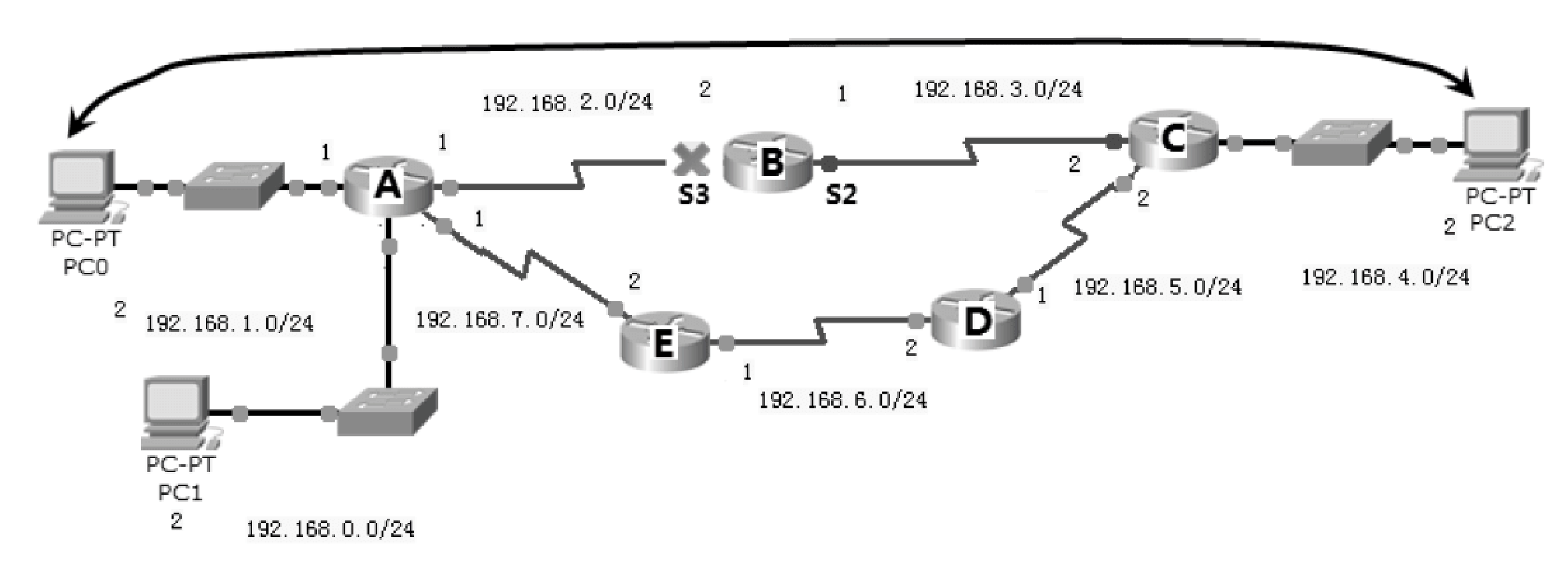
```
RC#show ip route
Gateway of last resort is not set
R    192.168.1.0/24 [120/2] via 192.168.3.1, 00:00:00, Serial2/0
R    192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:00, Serial2/0
C    192.168.3.0/24 is directly connected, Serial2/0
C    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.5.0/24 is directly connected, Serial3/0
R    192.168.6.0/24 [120/1] via 192.168.5.1, 00:00:13, Serial3/0
R    192.168.7.0/24 [120/2] via 192.168.5.1, 00:00:13, Serial3/0
                    [120/2] via 192.168.3.1, 00:00:00, Serial2/0
```

可以看到已经没有到 192.168.0.0/24 网段的路由了。

（9）在 PC0 上，跟踪数据包到 PC2 的路径。

```
PC>tracert 192.168.4.2
Tracing route to 192.168.4.2 over a maximum of 30 hops:
  1   22 ms     10 ms     5 ms      192.168.1.1     --路由器 A
  2   7 ms      7 ms      12 ms     192.168.2.2     --路由器 B
  3   12 ms     9 ms      11 ms     192.168.3.2     --路由器 C
  4   18 ms     15 ms     20 ms     192.168.4.2     --PC4
Trace complete.
```

可以看到这两个网段通信途径路由器 A、B 和 C。如图 6-4 所示，这是经过路由最少也就是跳数最少的路径，RIP 协议认为这是最佳路径，哪怕是 A 到 B 和 B 到 C 之间连接带宽是 56Kb/s，A 到 E、E 到 D、D 到 C 之间的连接带宽是 1000Mb/s，RIP 协议也认为 A-B-C 是最好的路径。因为 RIP 协议的度量值就是跳数，没有考虑带宽和延迟。



▲图 6-4　RIP 选择的最佳路径

（10）如图 6-4 所示，将路由器 B 的 S3 接口关闭，模拟该链路故障。看看 RIP 协议是否自动调整路由表，以保证网络畅通。

```
RB (config) #interface Serial 3/0
RB (config-if) #sh  --关闭端口
```

（11）在 PC0 上跟踪到达 PC2 的数据包路径。

```
PC>tracert 192.168.4.2
Tracing route to 192.168.4.2 over a maximum of 30 hops:
  1   18 ms     5 ms      6 ms      192.168.1.1    --路由器 A
  2   14 ms     14 ms     16 ms     192.168.7.2    --路由器 E
  3   32 ms     15 ms     25 ms     192.168.6.2    --路由器 D
  4   39 ms     19 ms     25 ms     192.168.5.2    --路由器 C
  5   25 ms     24 ms     57 ms     192.168.4.2    --PC2
```

可以看到，如果最佳路径不可用了，RIP 协议会自动选择次一点的路径。一旦最佳路径恢复，则会自动选择最佳路径。

6.2.2 RIPv1 和 RIPv2

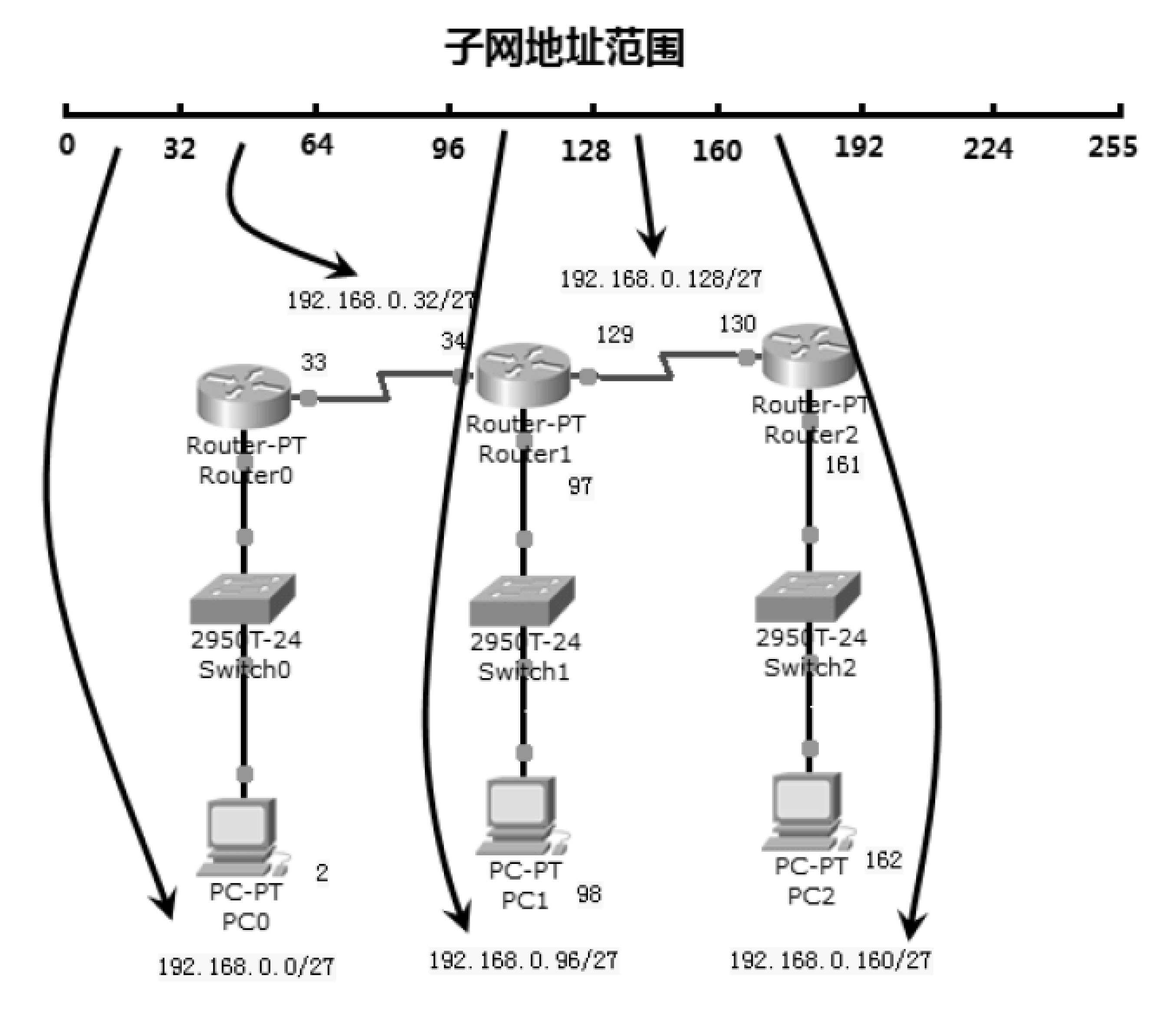
RIPv1 被提出较早，其中有许多缺陷。RIPv2 定义了一套有效的改进方案，新的 RIPv2 路由信息通告中包括子网掩码信息，所以支持变长子网，关闭自动汇总就支持不连续子网，组播方式发送路由更新报文，组播地址为 224.0.0.9，减少网络与系统资源的消耗，并提供了验证机制，增强了安全性。

下面为大家介绍什么是等长子网、变长子网和不连续子网。明白了这些，也就明白了什么时候用 RIPv1，什么情况下必须用 RIPv2。

1. 等长子网

等长子网就是将一个网络等分成几个网段，每个网段的子网掩码都一样。如图 6-5 所示，你有一个 C 类网络 192.168.0.0/24 地址可用，你的网络有 5 个网段，每个网段中计算机的数量最多 30 个。如果不考虑地址浪费，你可以将该 C 类网络等分为 8 个子网，可以拿出其中的任意五个子网分配给你的网络。

网络中的各个子网的子网掩码都一样，为 255.255.255.224，这就是等长子网的划分。

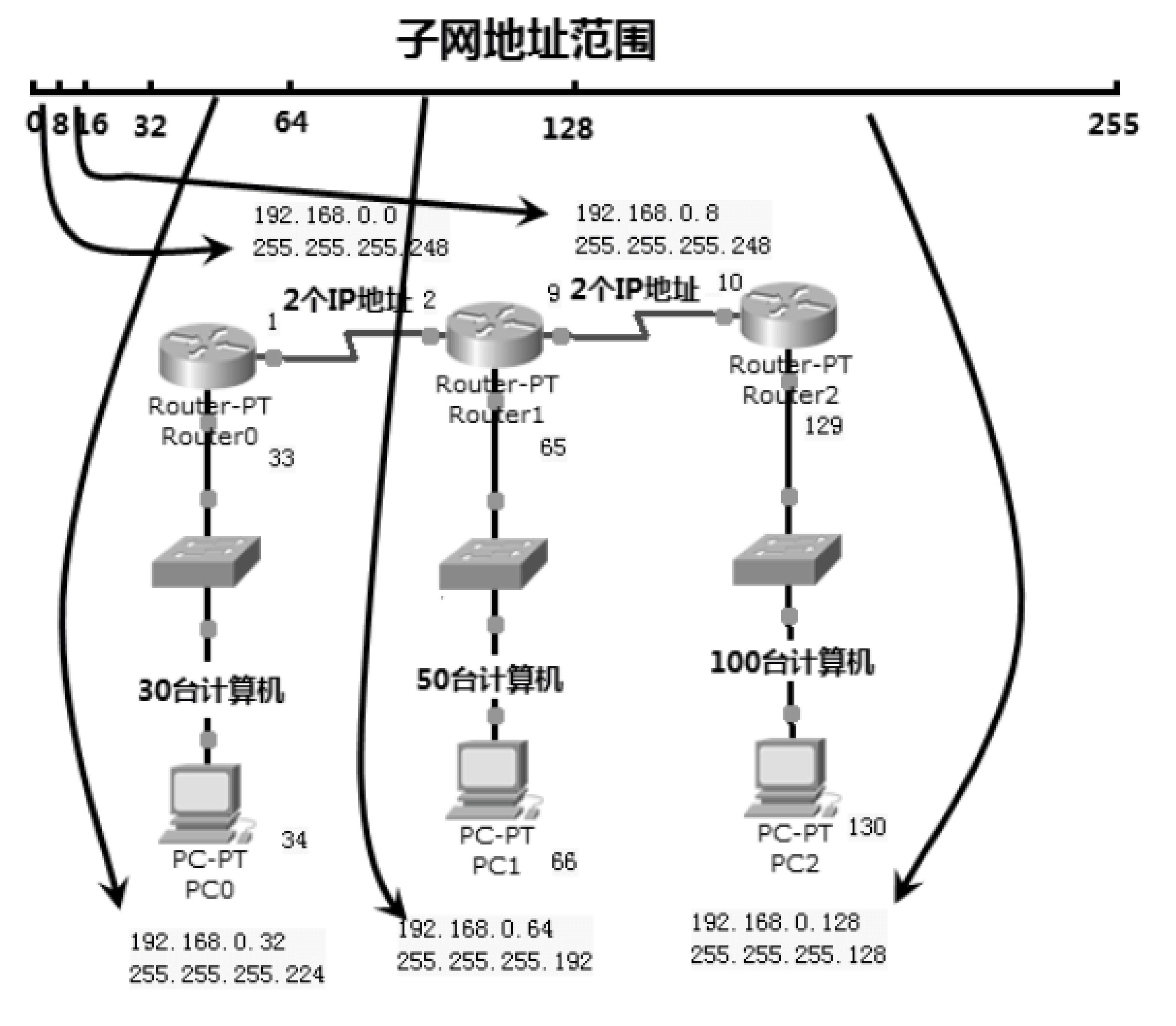


▲图 6-5　等长子网

RIPv1 支持等长子网划分。虽然 RIPv1 在交换路由信息时不包括子网掩码信息，但是网络中的路由器就以自己的子网掩码断定远程网段的子网掩码，所以它只支持等长子网。

2. 变长子网

如图 6-6 所示，网络中还是 5 个网络，其中一个网段需要部署 100 台计算机，一个网段需要部署 50 台计算机，一个网段需要部署 30 台计算机，路由器之间连接只需要两个 IP 地址。将一个 C 类网络 192.168.0.0/24 进行子网划分。子网地址范围和子网掩码如图中所示，每个网段的子网掩码不一样。



▲图 6-6　变长子网

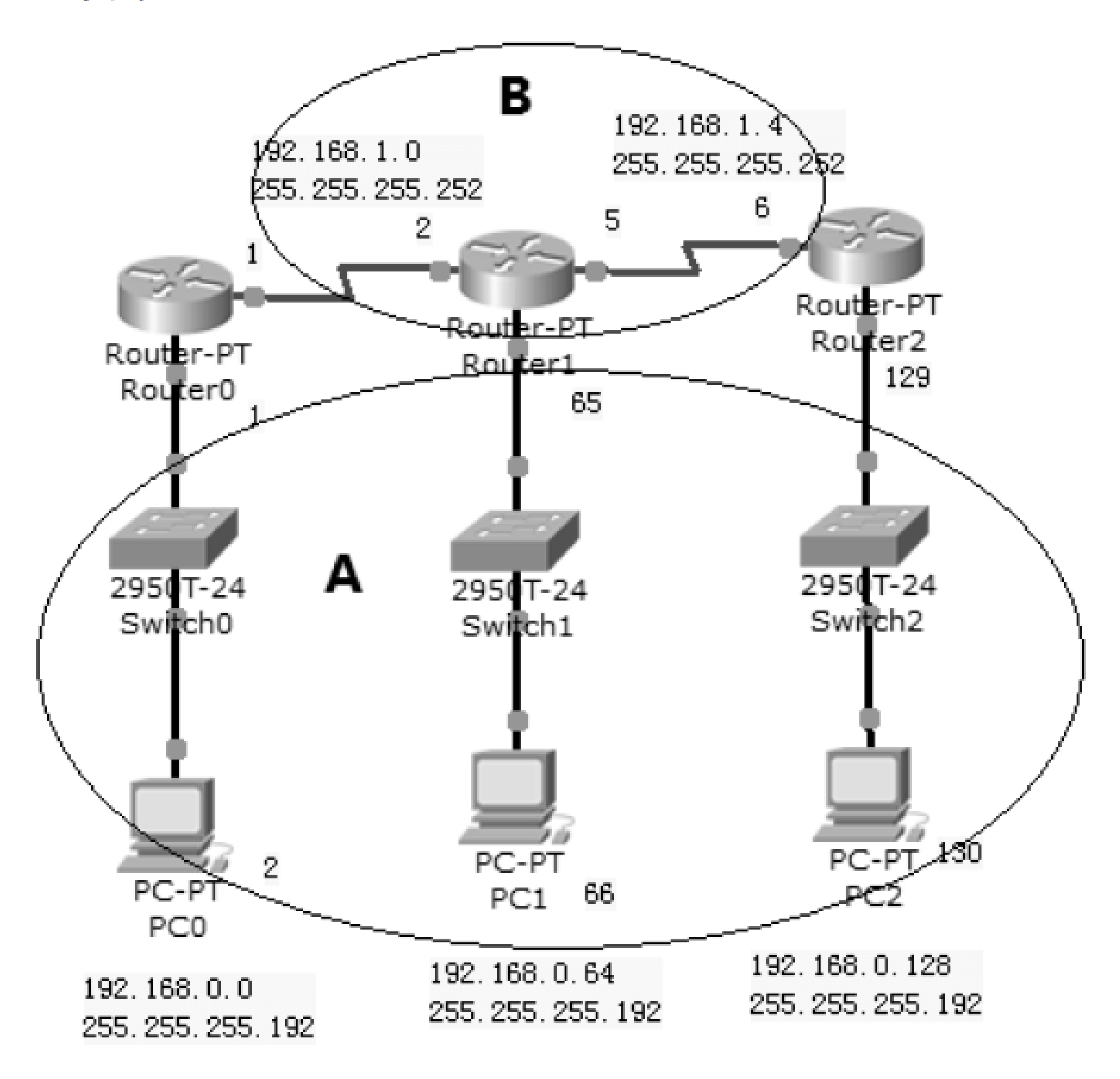
这就是变长子网，RIPv1 不支持变长子网。你需要明确将 RIP 的版本更改为 RIPv2，命令如下：

```
Router（config）#router rip
Router（config-router）#version 2
```

变长子网对应的实验为本章 6.7.1“实验 1：配置 RIPv2 支持变长子网”。

3．不连续子网

如图 6-7 所示，A 区域是 192.168.0.0/24 这个 C 类网络划分的子网。B 区域是 192.168.1.0/24 这个 C 类网络划分的子网。这就意味着 192.168.0.0/24 这个 C 类网络划分的子网被另一个 C 类网络隔开，就是不连续子网。



▲图 6-7　不连续子网

RIPv2 会自动在类的边界上汇总，也就是 Router0 向 Router1 通告路由信息时，直接告诉 Router1，我知道 192.168.0.0/24 网段如何转发。同时 Router2 向 Router1 通告路由信息时，直接告诉 Router1，我知道 192.168.0.0/24 网段如何转发。Router1 就会认为到 192.168.0.0/24 有两条可用的路径。很显然这是错误的。

要想让 RIPv2 支持不连续子网，必须关闭自动汇总。关闭自动汇总的命令如下：

```
Router (config) #router rip
Router (config-router) #version 2
Router (config-router) #no auto-summary
```

不连续子网对应的实验为本章 6.7.2 小节“实验 2：配置 RIPv2 支持不连续子网”。

6.3 EIGRP 协议

增强型内部网关路由选择协议 EIGRP（Enhanced Interior Gateway Routing Protocol）是 Cisco 的一个专用协议，它可以运行在 Cisco 路由器上。如果你的网络中有 Cisco 和华为两个厂商的路由器，你就不能使用 EIGRP 协议。由于 EIGRP 是目前两个最为流行的路由选择协议之一，因此，理解它对你来说是非常重要的。

EIGRP 是内部网关路由选择协议 IGRP（Interior Gateway Routing Protocol）的增强版，它们的关系类似于 RIPv2 和 RIPv1。EIGRP 支持变长子网，关闭路由汇总后支持不连续子网。

EIGRP 的特点如下。

- 使用 Hello 消息发现邻居，然后交换路由信息，使用 Hello 包维持邻居表。
- 有备用路径。当最佳路径不可用时，立即使用备用路径。
- 度量值默认为带宽和延迟，也可以添加负载、可靠性以及最大传输单元（MTU）。
- 默认支持 4 条链路的不等代价的负载均衡，可以更改为最多 6 条。
- 最大跳数为 255（默认是 100 跳）。
- 触发式更新路由表，即网络发生变化时，增量更新。
- 支持路由的自动汇总。
- 支持大的网络，可以使用自制系统号来区别可共享路由信息的路由器集合，路由信息只可以在拥有相同自制系统号的路由器间共享。
- 管理距离是 90。

EIGRP 支持邻居，这些邻居是通过 Hello 过程来发现的，并且邻居状态是要受监视的，像许多距离矢量协议一样，大部分路由器是绝不会了解到第一手路由更新的。

EIGRP 使用了一系列的表来保存这些关于环境的重要信息。

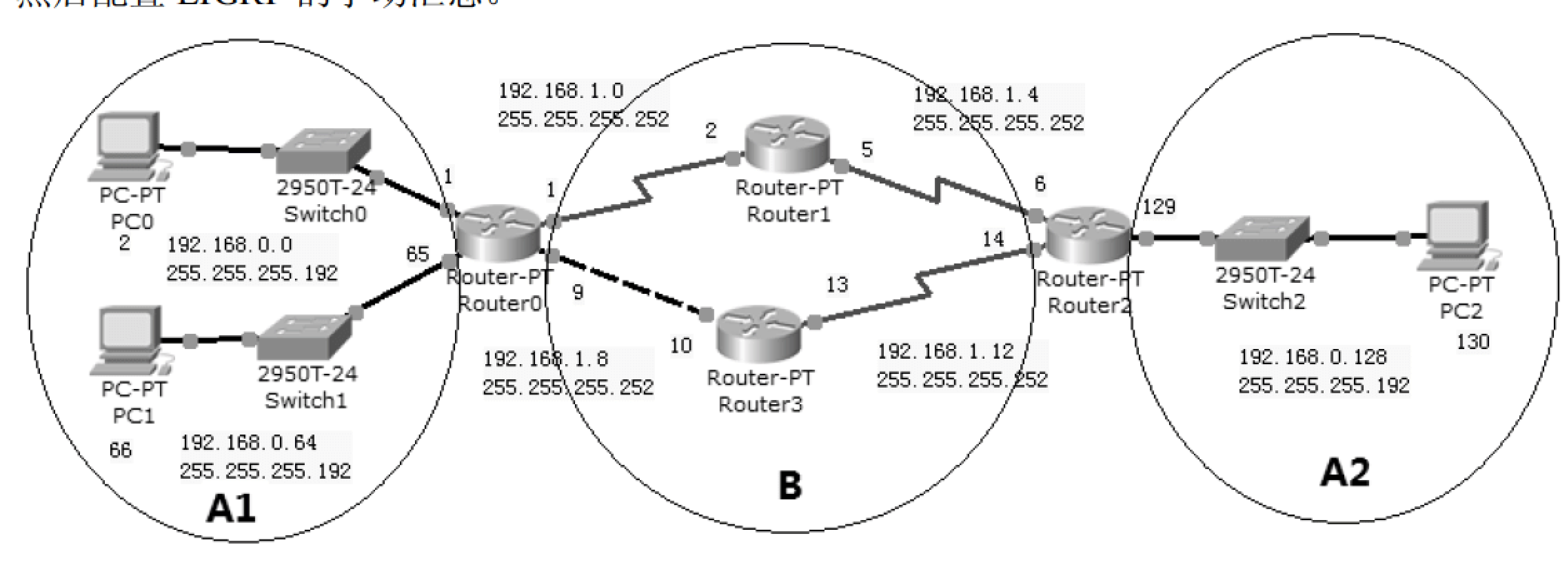
- 邻居关系表：邻居关系表（通常又称为邻居表）记录着有关路由器与已建立起来的邻居关系的信息。
- 拓扑表：拓扑表保存着在互联网络中每个路由器从每个邻居处接收到的路由通告。
- 路由表：路由表保存着当前使用着的用于路由判断的路由。

6.3.1 EIGRP 的配置过程

下面将会以实例演示 EIGRP 配置的过程，会讲解过程中使用的参数。

打开随书光盘中第 6 章练习“02 动态路由 EIGRP.pkt”，网络拓扑和 IP 地址规划如图 6-8 所示，网络中的路由器和 IP 地址已经配置好。Router0 和 Router3 之间使用快速以太网接口连接。

注意观察 IP 地址，其中 A1 和 A2 区域是 192.168.0.0/24 C 类网络划分的子网，中间的 B 区域是 192.168.1.0/24 C 类网络。对于 192.168.0.0/24 划分的子网就是不连续子网。EIGRP 协议会在 IP 地址类边界自动汇总。本实验需要关闭 EIGRP 的自动汇总来支持不连续子网，然后配置 EIGRP 的手动汇总。



▲图 6-8 网络拓扑

下面的步骤将会演示在这个网络中配置路由器使用 EIGRP 协议交换路由信息，查看路由表。

操作步骤如下。

（1）在 Router0 上，启用和配置 EIGRP。

```
Router>en
Router#config t
Router (config) #router eigrp 10   --这里的 10 是自制系统编号
Router (config-router) #network 192.168.0.0
Router (config-router) #network 192.168.1.0
```

这里的 10 是自制系统编号，本实验的所有路由器 EIGRP 自制系统编号都是 10，当然你也可以给其他的自制系统编号。不一样的自制系统不能交换路由信息和 Hello 数据包。后面的 network 的配置和 RIP 一样，是告诉路由器哪些端口连接的网段能够被 EIGRP 协议通告出去。

（2）在 Router1 上，启用和配置 EIGRP。

```
Router (config) #router eigrp 10
Router (config-router) #network 192.168.1.0
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.1 (Serial3/0) is up: new
```

```
        adjacency
```

发现邻居。

（3）在 Router2 上，启用和配置 EIGRP。

```
Router（config）#router eigrp 10
Router（config-router）#network 192.168.0.0
Router（config-router）#network 192.168.1.0
```

（4）在 Router3 上，启用和配置 EIGRP。

```
Router（config）#router eigrp 10
Router（config-router）#network 192.168.1.0
```

（5）在 Router0 上，查看路由表。

```
Router#show ip route
Gateway of last resort is not set
       192.168.0.0/24 is variably subnetted, 3 subnets, 2 masks
D      192.168.0.0/24 is a summary, 03:35:59, Null0    --在类的边界汇总
C      192.168.0.0/26 is directly connected, FastEthernet0/0
C      192.168.0.64/26 is directly connected, FastEthernet1/0
       192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
D      192.168.1.0/24 is a summary, 00:40:31, Null0    --在类的边界汇总
C      192.168.1.0/30 is directly connected, Serial2/0
D      192.168.1.4/30 [90/21024000] via 192.168.1.2, 03:29:35, Serial2/0
C      192.168.1.8/30 is directly connected, FastEthernet6/0
D      192.168.1.12/30 [90/20514560] via 192.168.1.10, 00:40:30,
       FastEthernet6/0
```

在上面显示的路由表中，D 开头的路由标明其是通过 EIGRP 协议构造的路由。可以看到，没有 192.168.0.128/26 这个子网，因为 EIGRP 协议默认在类的边界自动汇总。

（6）在 Router1 上，查看路由表。

```
Router#show ip route
Gateway of last resort is not set
D      192.168.0.0/24 [90/20514560] via 192.168.1.1, 03:29:22, Serial3/0
                [90/20514560] via 192.168.1.6, 00:49:46, Serial2/0
       192.168.1.0/30 is subnetted, 4 subnets
C      192.168.1.0 is directly connected, Serial3/0
C      192.168.1.4 is directly connected, Serial2/0
D      192.168.1.8 [90/20514560] via 192.168.1.1, 00:40:18, Serial3/0
D      192.168.1.12 [90/21024000] via 192.168.1.6, 00:49:46, Serial2/0
```

可以看到，在 Router1 上构造的路由表，到 192.168.0.0/24 网络有两条路径。很显然这种汇总是错误的。

下面将演示关闭自动汇总。

6.3.2 关闭 EIGRP 的自动汇总

关闭 EIGRP 协议的自动汇总，能够使之支持不连续子网。

在所有的路由器上运行以下命令关闭 EIGRP 的自动汇总。

```
Router (config) #router eigrp 10
Router (config-router) #no auto-summary
```

6.3.3 查看 EIGRP 的配置和路由表

在 Router1 上，查看 EIGRP 协议的配置，查看关闭自动汇总后的路由表，如图 6-9 所示。

```
Router#show ip route                    --查看关闭自动汇总后的路由表
```

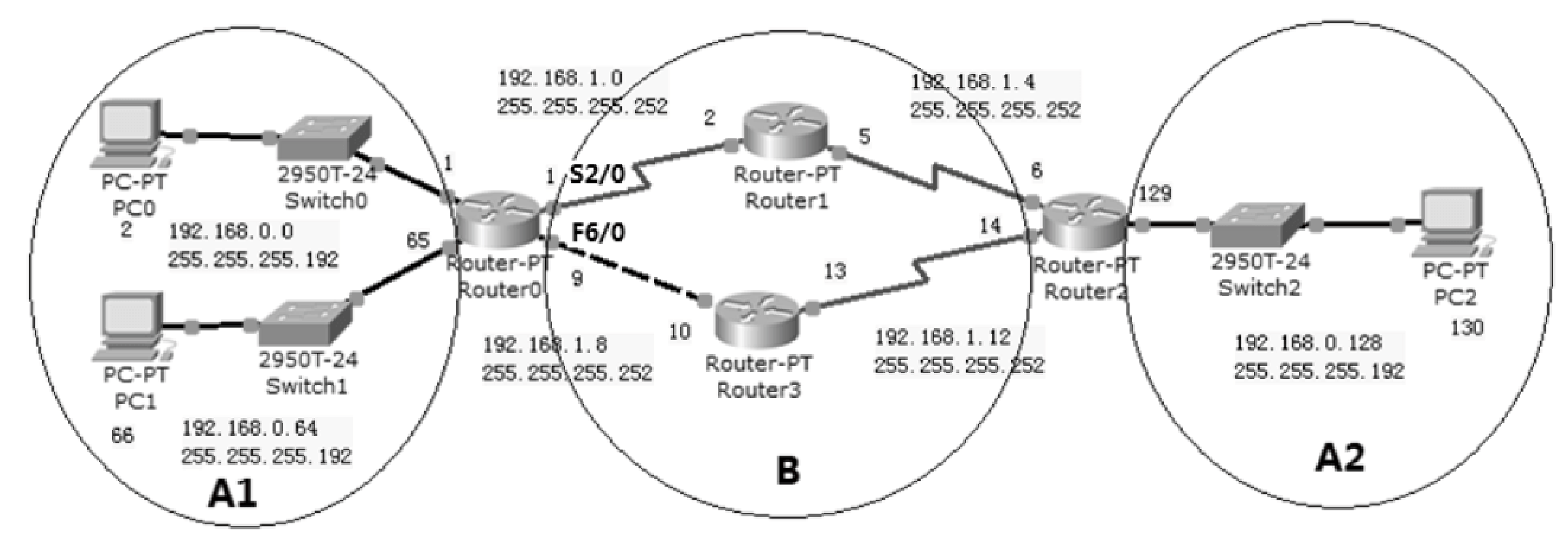
```
Router#show ip route
Gateway of last resort is not set
     192.168.0.0/26 is subnetted, 3 subnets   三个子网的子网掩码为 /26
D       192.168.0.0 [90/20514560] via 192.168.1.1, 00:00:15, Serial3/0
D       192.168.0.64 [90/20514560] via 192.168.1.1, 00:00:15, Serial3/0
D       192.168.0.128 [90/20514560] via 192.168.1.6, 00:00:16, Serial2/0
     192.168.1.0/30 is subnetted, 4 subnets
C       192.168.1.0 is directly connected, Serial3/0
C       192.168.1.4 is directly connected, Serial2/0
D       192.168.1.8 [90/20514560] via 192.168.1.1, 00:00:15, Serial3/0
D       192.168.1.12 [90/21024000] via 192.168.1.6, 00:00:16, Serial2/0
```

▲图 6-9　EIGRP 学习到的路由

现在能够看到路由表中出现了网络中到所有网段的路由。注意，中括号中，90 代表管理距离，后面的值是度量值，该度量值是带宽和延迟两个指标算出来的。

6.3.4 EIGRP 手动汇总

本实验的网络中，A1 区域的两个子网 192.168.0.0/26 和 192.168.0.64/26 可以汇总成一条路由 192.168.0.0/25。可以在 Router0 的 S2/0 和 F6/0 进行汇总，如图 6-10 所示。



▲图 6-10　网络拓扑

（1）在 Router0 上，手动汇总。

```
Router (config) #interface Serial 2/0
Router (config-if) #ip summary-address eigrp 10 192.168.0.0 255.255.255.128
Router (config-if) #ex
Router (config) #interface fastEthernet 6/0
Router (config-if) #ip summary-address eigrp 10 192.168.0.0 255.255.255.128
```

（2）在 Router1 上，查看汇总的结果，如图 6-11 所示。

```
Router#show ip route
```

```
Router#show ip route
Gateway of last resort is not set   可以看到将A1区域中的两个子网汇总为一条路由
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.0.0/25 [90/20514560] via 192.168.1.1, 00:01:25, Serial3/0
D       192.168.0.128/26 [90/20514560] via 192.168.1.6, 00:12:36, Serial2/0
     192.168.1.0/30 is subnetted, 4 subnets
C       192.168.1.0 is directly connected, Serial3/0
C       192.168.1.4 is directly connected, Serial2/0
D       192.168.1.8 [90/20514560] via 192.168.1.1, 00:01:25, Serial3/0
D       192.168.1.12 [90/21024000] via 192.168.1.6, 00:12:36, Serial2/0
```

▲图 6-11　汇总结果

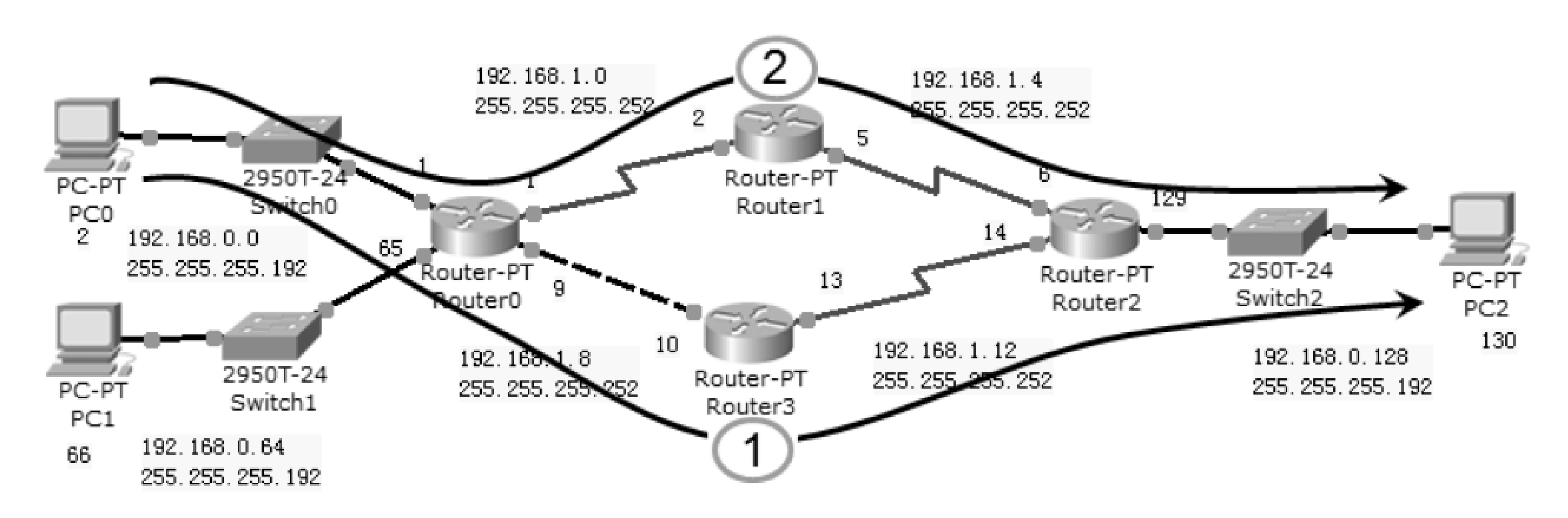
6.3.5　确认 EIGRP 选择的最佳路径

在 PC0 上跟踪到 PC2 的数据包传递路径。

```
PC>tracert 192.168.0.130
Tracing route to 192.168.0.130 over a maximum of 30 hops:
  1   3 ms     12 ms     8 ms     192.168.0.1        --Router0
  2   20 ms    15 ms     17 ms    192.168.1.10       --Router3
  3   25 ms    15 ms     17 ms    192.168.1.14       --Router2
  4   28 ms    21 ms     26 ms    192.168.0.130      --PC2
Trace complete.
```

如图 6-12 所示，根据数据包跟踪结果可知，EIGRP 协议在 192.168.0.0/26 网段到 192.168.0.128/26 网段的最佳路径是①，路径②是备用路径。

下面讲解如何查看 EIGRP 的备用路径。



▲图 6-12　备用路径

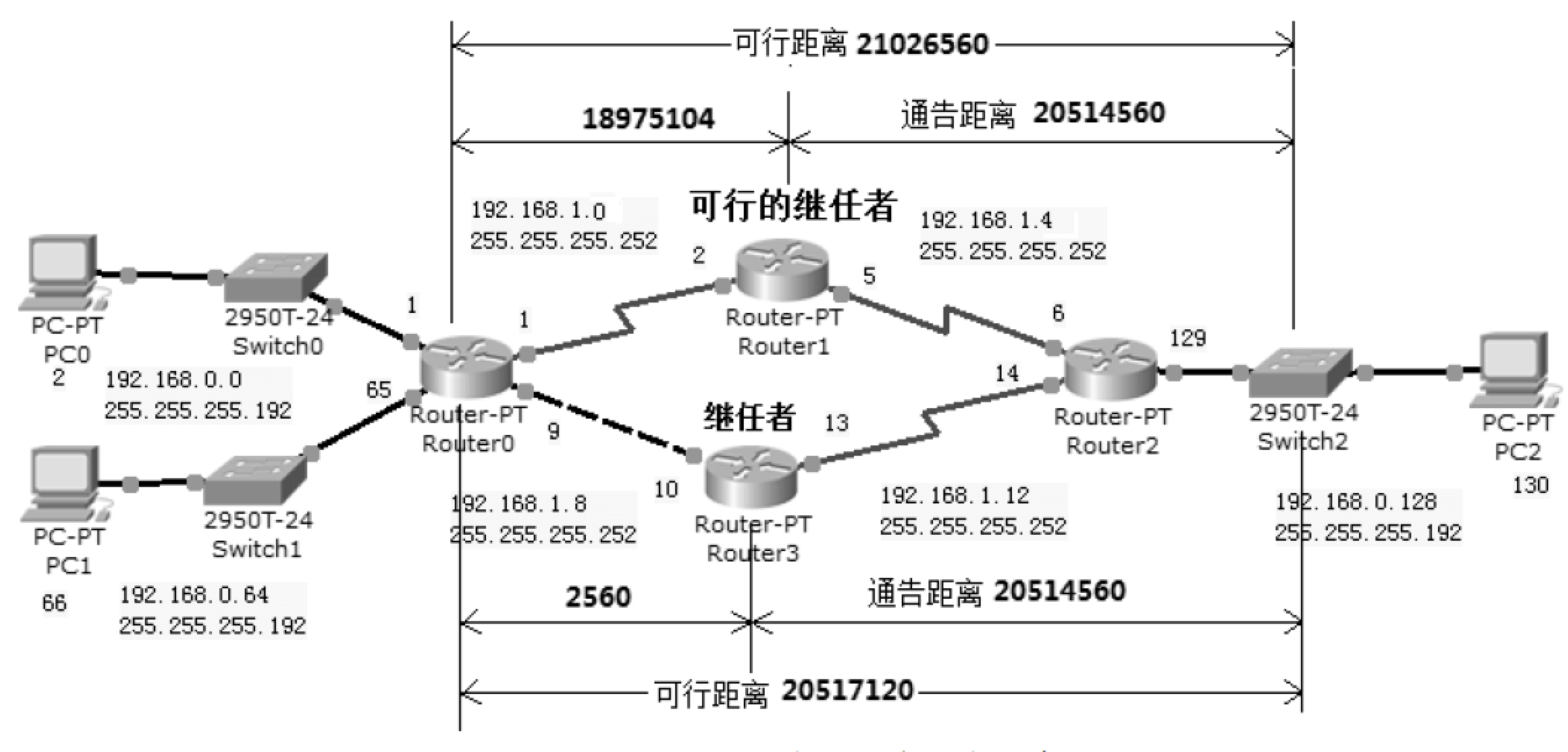
6.3.6 查看 EIGRP 的备用路径

使用 show ip eigrp topology 命令可以查看备用路径。以下命令在 Router0 上运行。

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for AS 10
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
      r - Reply status
P 192.168.0.0/26, 1 successors, FD is 28160
       via Connected, FastEthernet0/0
P 192.168.0.64/26, 1 successors, FD is 28160
       via Connected, FastEthernet1/0
P 192.168.1.0/30, 1 successors, FD is 20512000
       via Connected, Serial2/0
P 192.168.1.4/30, 1 successors, FD is 21024000
       via 192.168.1.2 (21024000/20512000), Serial2/0
P 192.168.1.12/30, 1 successors, FD is 20514560
       via 192.168.1.10 (20514560/20512000), FastEthernet6/0
P 192.168.1.8/30, 1 successors, FD is 28160
       via Connected, FastEthernet6/0
P 192.168.0.128/26, 1 successors, FD is 20517120   --到该网段有一个最佳路径
      via 192.168.1.10 (20517120/20514560), FastEthernet6/0
                                                        --该路径是最佳路径
      via 192.168.1.2 (21026560/20514560), Serial2/0 --该路径是备用路径
```

注意 每个路由前面都有一个 P，这表明此路由处于被动状态。这是一件好事情，因为激活状态（A）的路由，指示该路由器已经失去了它到这个网络的路径，并且正在搜索替代路径。每个表项也标识了到远程网络加上下一跳邻居可行的距离，这个下一跳邻居是指数据包将通过它被传输到目标网络。这里说的距离是带宽和延迟两个指标算出来的度量值，该值越小，距离越短。

在圆括号中，每个表项还有两个数值，第一个数值指示可行距离，而第二个是到达远程网络的通告距离。如图 6-13 所示，Router1 通告 Router0，它到 192.168.0.128/26 网段的距离是 20514560，这就是通告距离，Router0 计算到达该网络的距离需要在通告距离的基础上加上它到 Router1 的距离，这就是可行距离。虽然 Router1 和 Router3 通告给 Router0 的距离相同，但是由于 Router0 到 Router3 之间是以太网连接，距离短，因此 Router3 成为继任者，而 Router1 成为可行的继任者（备份路由）。但只有一个继任路由（那个具有最低度量的）将会被复制并放入到路由表中。



▲图 6-13　可行距离和通告距离示意图

6.3.7　查看 EIGRP 邻居

在任何路由上，运行以下命令可以查看 EIGRP 的邻居。

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address      Interface    Hold Uptime    SRTT   RTO    Q    Seq
                                  (sec)             (ms)        Cnt  Num
0   192.168.1.10     Fa6/0     10    02:02:28   40     1000   0    85
1   192.168.1.2      Se2/0     13    02:02:28   40     1000   0    76
```

以上命令可以显示 EIGRP 的邻居，如果你发现邻居缺少，就应该检查相邻的路由器是否正确配置了 EIGRP、自制系统编号是否相同、是否正确地配置了 network。

6.3.8　显示 EIGRP 协议活动

debug eigrp packets 可以显示出在两台相邻路由器间所发送的 Hello 数据包。

```
Router#debug eigrp packets
EIGRP: Sending HELLO on FastEthernet0/0
  AS 10, Flags 0x0, Seq 76/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on FastEthernet6/0
  AS 10, Flags 0x0, Seq 76/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on Serial2/0
  AS 10, Flags 0x0, Seq 76/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Received HELLO on Serial2/0 nbr 192.168.1.2
```

```
  AS 10, Flags 0x0, Seq 77/0 idbQ 0/0
EIGRP: Sending HELLO on FastEthernet1/0
  AS 10, Flags 0x0, Seq 76/0 idbQ 0/0 iidbQ un/rely 0/0
Router#undebug all    --关闭诊断输出，也可输入 un all 关闭诊断输出
```

Hello 数据包会送到每个激活的接口上，也就是那些有邻居相连接的接口，并由这些接口送出。你是否注意到在这个更新中提供的 AS 号？要知道，如果某个邻居没有相同的 AS 号，它所发出的 Hello 更新将会被丢弃。

```
Router #debug ip eigrp notification
```

在平时这个命令的输出根本不能告诉你任何有价值的事情！只有当你的网络出现问题时，或者在你的互联网络中从某台路由器上添加或删除了一个网络时，它才是有价值的。该命令在 packet tracer 软件中没有提供。

6.3.9　更改 EIGRP 的默认设置

默认时，EIGRP 支持最多 4 条链路的不等价路径的负载均衡，通过以下命令可以使 EIGRP 支持 6 条等价或不等价负载均衡链路。默认最大跳数 100，可以被设置到 255。Packet Tracer 软件模拟的路由器不支持以下命令。

```
Router (config) #router eigrp 10
Router (config-router) #maximum-path ?
<1-6> Number of paths
Router (config-router) #metric maximum-hops ?
<1-255> Hop Count
```

EIGRP 的课后实验为本章 6.7.3 小节“实验 3：配置 EIGRP 手动汇总”。

6.4　OSPF 协议

开放最短路径优先 OSPF（Open Shortest Path First）是一个开放标准的路由选择协议，它被各种网络开发商所广泛使用，其中包括 Cisco。如果你的网络拥有多种路由器，而并不全都是 Cisco 的，那么你将不能使用 EIGRP，那你可以用什么呢？基本上剩下的也只有 RIPv1、RIPv2 或 OSPF。如果你的网络是一个大型网络，那么你真正的选择就只能是 OSPF 和被称为路由再发布的服务了，即能在路由选择协议之间提供转换的服务。

OSPF 是通过使用 Dijkstra 算法来工作的。首先，构建一个最短路径树，然后使用最佳路径的计算结果来组建路由表。OSPF 汇聚很快，虽然它可能没有 EIGRP 快，并且它也支持到达相同目标的多个等开销路由，但与 EIGRP 一样，它支持 IP 和 IPv6。

OSPF 协议具有下列特性。

- 由区域和自治系统组成。
- 最小化的路由更新的流量。

- 允许可缩放性。
- 支持变 VLSM 和 CIDR。
- 拥有不受限的跳数。
- 允许多销售商的设备集成（开放的标准）。
- 度量值是带宽。

6.4.1 OSPF 相关术语

在学习 OSPF 之前，先要介绍一下与之相关的术语。

- 链路：链路就是指定给任一给定网络的一个网络或路由器接口。当一个接口被加入到该 OSPF 的处理中时，它就被 OSPF 认为是一个链路。这个链路或接口，将有一个指定给它的状态信息（up 或 down，即激活或失效），以及一个或多个 IP 址。
- 路由器 ID：路由器 ID（RID）是一个用来标识此路由器的 IP 地址。Cisco 通过使用所有被配置的环回接口中最高的 IP 地址，来指定此路由器 ID。如果没有带有地址的环回接口被配置，OSPF 将选择所有激活的物理接口中最高的 IP 地址为其 RID。
- 邻居：邻居可以是两台或更多的路由器，这些路由器都有某个接口连接到一个公共的网络上，如两台连接在一个点到点串行链路上的路由器。
- 邻接：邻接是两台 OSPF 路由器之间的关系，这两台路由器允许直接交换路由更新数据。OSPF 对于共享的路由选择信息是非常讲究的，不像 EIGRP 那样直接地与自己所有的邻居共享路由信息。OSPF 只与建立了邻接关系的邻居直接共享路由信息，并不是所有的邻居都可以成为邻接，这将取决于网络的类型和路由器上的配置。
- Hello 协议：OSPF 的 Hello 协议可以动态地发现邻居，并维护邻居关系。Hello 数据包和链路状态通告（LSA）建立并维护着拓扑数据库。Hello 数据包的地址是 224.0.0.5。
- 邻居关系数据库：邻居关系数据库是一个 OSPF 路由器的列表，这些路由器的 Hello 数据包是可以被相互看见的。每台路由器上的邻居关系数据库管理着各种详细资料，如路由器 ID 和状态。
- 拓扑数据库：拓扑数据库中包含来自所有从某个区域接收到的链路状态通告信息。路由器使用这些来自拓扑数据库中的信息作为 Dijkstra 算法的输入，并为每个网络计算出最短路径。
- 链路状态通告：链路状态通告（LSA）是一个 OSPF 的数据包，它包含在 OSPF 路由器中共享的链路状态和路由信息。有多种不同类型的 LSA 数据包。OSPF 路由器将只与建立了邻接关系的路由器交换 LSA 数据包。
- 指定路由器：无论什么时候，当 OSPF 路由器被连接到相同的多路访问型的网络时，都需要选择一台指定路由器（DR）。Cisco 喜欢将这些网络称为“广播” 网络，这些网络上拥有多个接收者。不要将多路访问与多连接点混淆，有时它们是不易被区分开的。

一个典型的示例是以太型 LAN。为了最小化所需构成的邻接数量，被选择（挑选）的

DR 将负责分发、收集路由选择信息到来自此广播网络或链路中的其他路由器上。这就确保了所有路由器上的拓扑表是同步的。这个共享网络中的所有路由器都将与 DR 和备用指定路由器（BDR）建立邻接关系。具有高优先级的路由器将胜出，成为 DR，当具有较高优先级的路由器都退出时，路由器的 ID 将打破平局的条件，即在具有相同优先级的路由器中选择 DR 时，拥有最高路由器 ID 的路由器将被选中。

- 备用指定路由器：备用指定路由器（BDR）是多路访问链路（记住，Cisco 有时喜欢称之为“广播”网络）上跃跃欲试的待命 DR。BDR 将从 OSPF 邻接路由器上接收所有的路由更新，但并不随便转发这些 LSA 更新。
- OSPF 区域：一个 OSPF 区域是一组相邻的网络和路由器。在同一区域内的路由器共享一个公共的区域 ID。由于路由器可以同时是多个区域中的成员，因此区域 ID 被指定给此路由器上特定的接口。这样，路由器上的某些接口可能属于区域 1，而剩下的接口则可能属于区域 0。所有在同一区域中的路由器拥有相同的拓扑表。在配置 OSPF 时需要记住，必须使用区域 0，在连接到网络主干的路由器上时，它通常是要被配置的。区域在建立一个分级的网络组织中扮演着重要的角色，它真正强化了 OSPF 的可缩放性。
- 广播（多路访问）：广播（多路访问）网络就像以太网，它允许多台设备连接（或者是访问）到同一个网络，它是通过投递单一数据包到网络中所有的结点来提供广播能力的。在 OSPF 中，每个广播（多路访问）网络都必须选出一个 DR 和一个 BDR。
- 非广播的多路访问：非广播的多路访问（NBMA）网络是那些像帧中继、X.25 和异步传输模式（ATM）类型的网络。这些网络允许多路访问，但不拥有如以太网那样的广播能力。因此，为实现恰当的功能，NBMA 网络需要特殊的 OSPF 配置，并且必须详细定义邻居关系。
- 点到点：点到点被定义为一种包含两台路由器间直接连接的网络拓扑类型，这一连接为路由器提供了单一的通信路径。点到点连接可能是物理的，比如直接连接两台路由器的串行电缆；它也可以是逻辑的，如通过帧中继网络电路在两台相隔上千英里的路由器间形成的连接。无论怎样，这种类型的配置排除了对 DR 或 BDR 的需求，并且它们邻居关系的发现也是自动完成的。
- 点到多点：点到多点也被定义为是一种网络的拓扑类型，这种拓扑包含有路由器上的某个单一接口与多个目的路由器间的一系列连接。这里，所有路由器的所有接口都共享这个属于同一网络的点到多点的连接。与点到点一样，这里不需要 DR 或 BDR。

在理解 OSPF 的操作过程时，所有这些术语都扮演着一个重要的角色。因此，需要再一次确信你已经非常熟悉它们当中的每一个。仔细阅读本章的后续内容，将会帮助你在恰当的上下文中找出这些术语的位置。

6.4.2 支持多区域

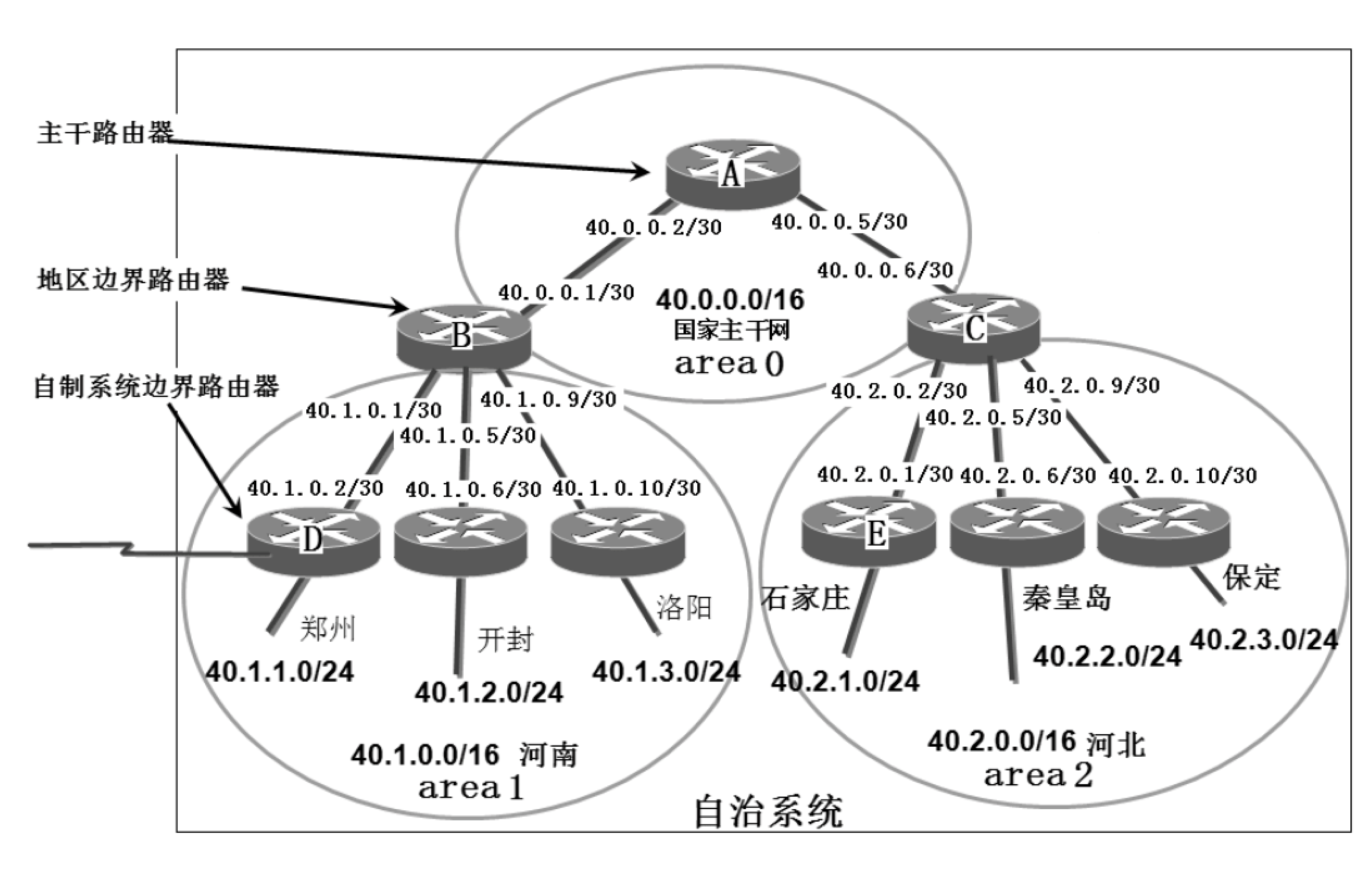
OSPF 是一个快速的、可缩放的和高效能的协议，进而可以被应用在有数以千计的路由

设备的大规模网络中。OSPF 设计用于分层的结构中，使用 OSPF 可以将大型互联网络分割成一些小的被称为区域的小互联网络，这是 OSPF 协议设计中的精华。

将 OSPF 协议创建为层次结构的原因如下。

- 减少路由选择的开销。
- 加速汇聚。
- 用单一的网络区域来缩小网络的不稳定性。

如图 6-14 所示，河北省分配的地址段为 40.2.0.0/16，河南省分配的地址段为 40.1.0.0/16，国家主干网分配的地址段为 40.0.0.0/16。国家主干网作为 OSPF 的 area 0，可以将一个省作为一个 OSPF 区域，这些区域和 area 0 相连。



▲图 6-14　OSPF 多区域与地址规划

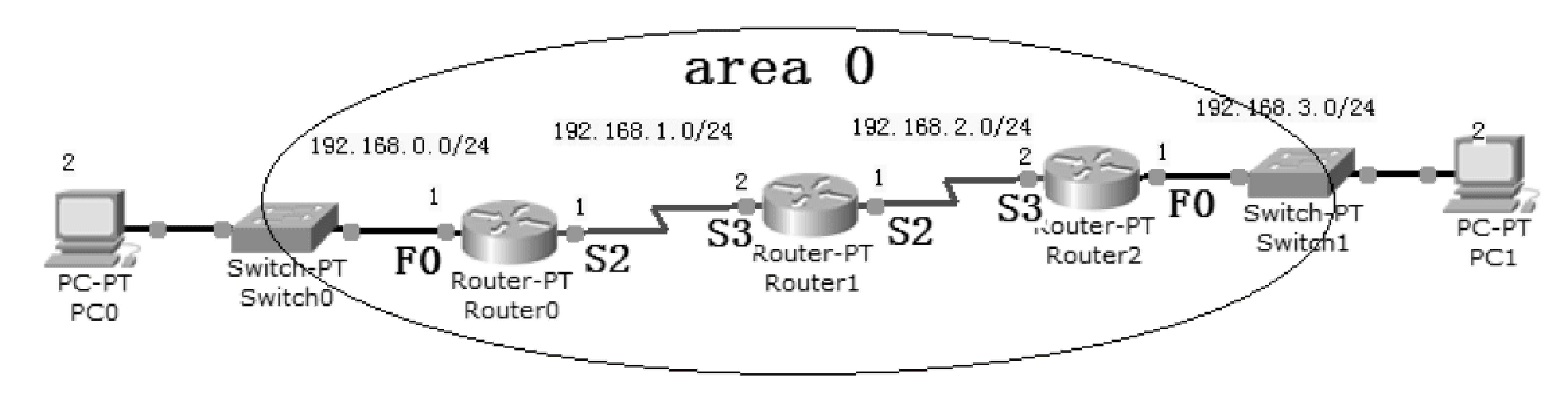
路由器 B 可以将 area 1 的网络汇总成一条通告给 area 0，路由器 C 可以将 area 2 的网络汇总成一条通告给 area 0。比如保定网络的某个接口 up 或 down 只会引起 area 2 网络中的路由器交换链路状态，重新计算路由表；对 area 0 和 area 1 中的网络没有任何影响。这样就将网络的不稳定造成的影响，控制在一个 area。

图 6-14 给出了典型的 OSPF 简易设计。注意每台路由器是如何连接到主干网上的，此主干网被称为区域 0，或主干区域。OSPF 协议必须要有一个区域 0。而且如果可能，所有的路由器都应该连接到这个区域（那些没有直接连接到区域 0 的区域可以通过使用虚拟链路进行连接，但这一部分内容超出本书的范畴）。而那些在一个 AS 内部连接其他区域到此主干网的路由器，被称为区域边界路由器（ABR）。这些路由器至少有一个接口必须在区域 0 中。

6.4.3 OSPF 的 network 参数

与 RIP 和 EIGRP 一样，在启用了 OSPF 协议后，同样需要使用 network 命令标识 OSPF 将操作的接口。但是与 RIP 和 EIGRP 不同，后面需要指明通配符掩码和 OSPF 区域。

如图 6-15 所示，Router0、Router1 和 Router2 都属于 area 0。



▲图 6-15 网络拓扑

在 Router1 上配置 OSPF 的命令如下。

```
Router1 (config) #router ospf 1   --后面的值是进程 ID，可以是 1～65535 之间任何值
Router1 (config-router) #network 192.168.1.0 0.0.0.255 area 0
Router1 (config-router) #network 192.168.2.0 0.0.0.255 area 0
```

network 命令的参数是网络号（192.168.1.0）和通配符掩码（0.0.0.255），这两个数字的组合用于标识 OSPF 将操作的接口，并且它也将被包含在其 OSPF LSA 的通告中。OSPF 将使用这个命令来找出包括在 192.168.1.0/24 网络中的任何地址，它将会把找到的接口放置到 area 0 中。

在通配符掩码中，值为 0 的八位位组表示网络地址中相应的八位位组必须严格匹配，255 则表示不必关心网络地址中相应的八位位组的匹配情况。如 network 192.168.1.2 0.0.0.0 的组合将指定一个 192.168.1.2，而不包含其他地址。如果你想在指定接口上激活 OSPF，这种方式确实很有用，并且这也是完成这一工作可采用的非常明确且简单的方式。如果你坚持要匹配网络中的某个范围，则网络和通配符掩码 192.168.1.0 0.0.0.255 的组合将指定一个范围 192.168.1.0～192.168.1.255。由此可知，使用通配符掩码 0.0.0.0 将分别标识出每个 OSPF 的接口，它的确是一个比较简单且安全的方式。

在 Router1 上，由于接口 S2 和 S3 都属于 area 0，你也可以将这两个网段合并为一个。

```
Router1 (config) #router ospf 1
Router1 (config-router) #network 192.168.0.0 0.0.255.255 area 0
```

这就意味着，只要路由器的接口 IP 地址是 192.168 开头的，都将运行 OSPF，这些接口都属于 area 0。

如果这两个接口属于不同 area，你必须写两条 network 才能区分哪些接口属于哪个 area。

```
Router1 (config) #router ospf 1
Router1 (config-router) #network 192.168.1.0 0.0.0.255 area 1
Router1 (config-router) #network 192.168.2.0 0.0.0.255 area 0
```

最后的参数是区域号码，它指示网络中接口被标识以及通配符掩码所限定的区域。记住，

如果 OSPF 路由器的接口共享有相同区域号的网络，那么这些路由器将完全可以成为邻居。区域号可以是 1～4 294 967 295 范围内的十进制数，也可以被表示为标准的点分符号的数值。例如，区域 0.0.0.0 是一个合法的区域，它也可以同样表示为区域 0。

6.4.4 配置 OSPF 单区域

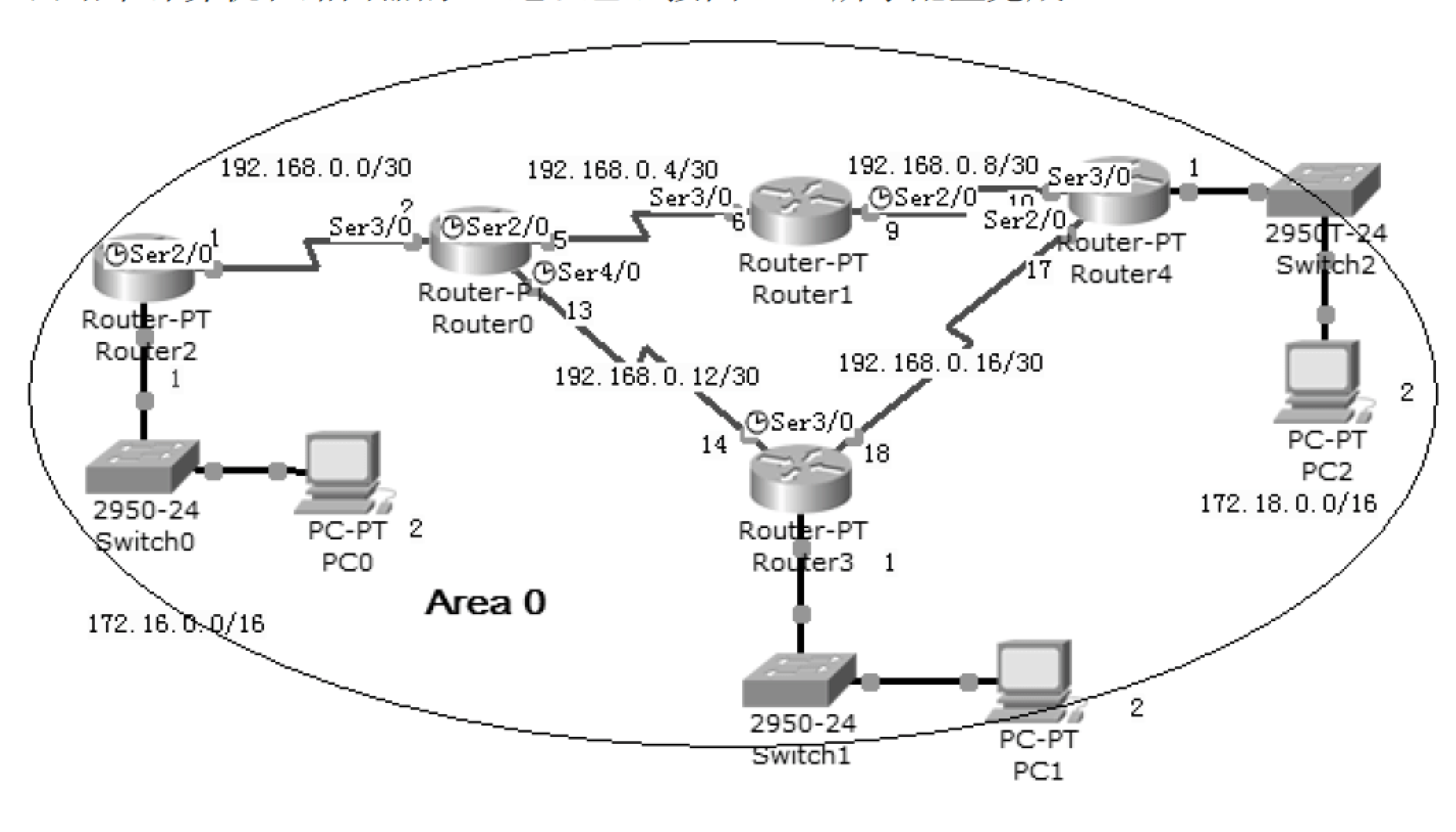
打开随书光盘中第 6 章练习“03　OSPF 单区域.pkt”，网络拓扑和 IP 地址如图 6-16 所示。

1．实验目的

能够在单区域环境中配置 OSPF 路由协议。

2．网络拓扑和实验环境

网络中计算机和路由器的 IP 地址已经按图 6-16 所示配置完成。



▲图 6-16　网络拓扑

3．实验要求

- 在 Area 0 中配置 OSPF。
- 查看路由表。
- 检查 OSPF 协议的收敛速度。

4．操作步骤

（1）在 Router2 上，配置 OSPF 协议。

```
Router>en
Router#config t
```

```
Router (config) #router ospf 1
Router (config-router) #network 192.168.0.0 0.0.0.3 area 0
Router (config-router) #network 172.16.0.0 0.0.255.255 area 0
```

（2）在 Router0 上，配置 OSPF 协议。

```
Router (config) #router ospf 100          --进程 ID 可以和其他路由器的不一样
Router (config-router) #network 192.168.0.0 0.0.0.3 area 0
Router (config-router) #network 192.168.0.4 0.0.0.3 area 0
Router (config-router) #network 192.168.0.12 0.0.0.3 area 0
Router (config-router) #ex
```

> **注意** 通配符掩码，其实就是子网掩码的反转，即子网掩码的 1 变成 0，0 变成 1。如果某个网段的子网掩码是 255.255.255.252，二进制位 11111111. 11111111. 11111111. 11111100，那么它的反转源码为 00000000. 00000000. 00000000. 00000011，即 0.0.0.3。

以上的配置可以使用下面的命令代替，反转掩码为 0.0.0.255，意味着只要 IP 地址是 192.168.0 的接口都运行 OSPF 协议，且都工作在 area 0。

```
Router (config) #router ospf 100
Router (config-router) #network 192.168.0.0 0.0.0.255 area 0
```

（3）在 Router1 上，配置 OSPF 协议。

```
Router (config) #router ospf 1
Router (config-router) #network 192.168.0.0 0.0.0.255 area 0
```

（4）在 Router4 上，配置 OSPF 协议。

```
Router (config) #router ospf 1
Router (config-router) #network 192.168.0.0 0.0.0.255 area 0
Router (config-router) #network 172.18.0.0 0.0.255.255 area 0
```

（5）在 Router3 上，配置 OSPF 协议。

```
Router (config) #router ospf 1
Router (config-router) #network 192.168.0.0 0.0.0.255 area 0
Router (config-router) #network 172.17.0.0 0.0.255.255 area 0
```

6.4.5　检查路由表

（1）在 Router3 上，查看路由表。

```
Router#show ip route
Gateway of last resort is not set
O    172.16.0.0/16 [110/1563] via 192.168.0.13, 00:01:15, Serial2/0
C    172.17.0.0/16 is directly connected, FastEthernet0/0
```

```
O    172.18.0.0/16 [110/782] via 192.168.0.17, 00:01:15, Serial3/0
     192.168.0.0/30 is subnetted, 5 subnets
O    192.168.0.0 [110/1562] via 192.168.0.13, 00:01:15, Serial2/0
O    192.168.0.4 [110/1562] via 192.168.0.13, 00:01:15, Serial2/0
O    192.168.0.8 [110/1562] via 192.168.0.17, 00:01:15, Serial3/0
C    192.168.0.12 is directly connected, Serial2/0
C    192.168.0.16 is directly connected, Serial3/0
```

（2）查看 OSPF 邻居。

```
Router#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address         Interface
192.168.0.13      1    FULL/-          00:00:39    192.168.0.13    Serial2/0
192.168.0.17      1    FULL/-          00:00:35    192.168.0.17    Serial3/0
```

6.4.6 查看 OSPF 链路状态数据库

```
Router#show ip ospf database
          OSPF Router with ID （192.168.0.18） （Process ID 1）
             Router Link States （Area 0）
Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.0.1     192.168.0.1     673         0x80000005 0x0082b6 3
192.168.0.9     192.168.0.9     317         0x80000004 0x004015 4
192.168.0.17    192.168.0.17    219         0x80000005 0x00dc82 5
192.168.0.13    192.168.0.13    214         0x80000006 0x00fbd0 6
192.168.0.18    192.168.0.18    200         0x80000005 0x0093be 5
```

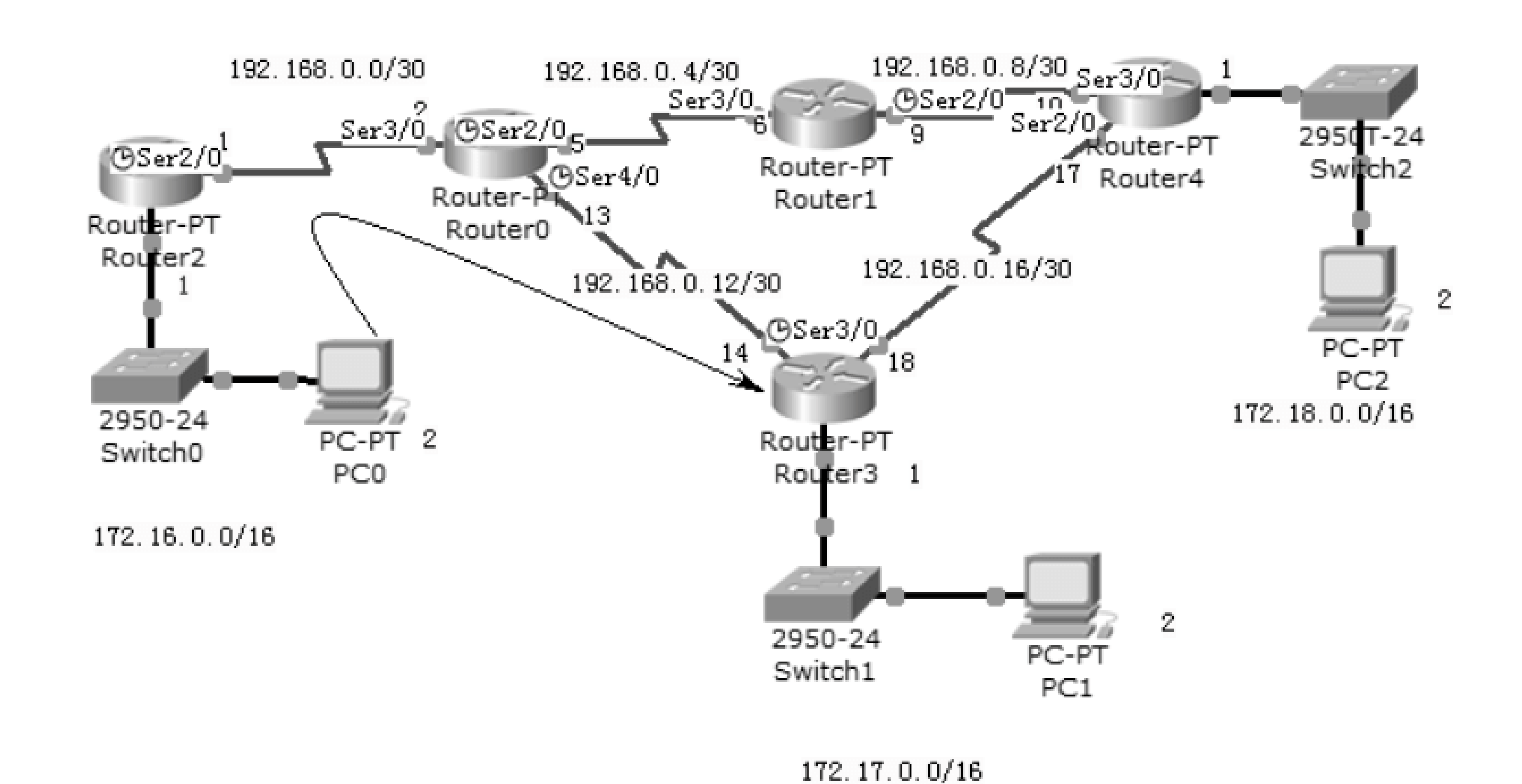
6.4.7 测试 OSPF 收敛速度

收敛速度，反映网络有变化后，网络中路由器上的路由表重新达到一致状态所需的时间。

（1）在 PC0 上，跟踪数据包路径。

```
PC>tracert 172.17.0.2
Tracing route to 172.17.0.2 over a maximum of 30 hops:
  1   6 ms      8 ms     7 ms      172.16.0.1
  2   12 ms     11 ms    11 ms     192.168.0.2
  3   13 ms     18 ms    15 ms     192.168.0.14
  4   25 ms     28 ms    29 ms     172.17.0.2
```

可以看到数据包是通过 Router2→Router0→Router3，如图 6-17 所示。



▲图 6-17　OSPF 选择的最佳路径

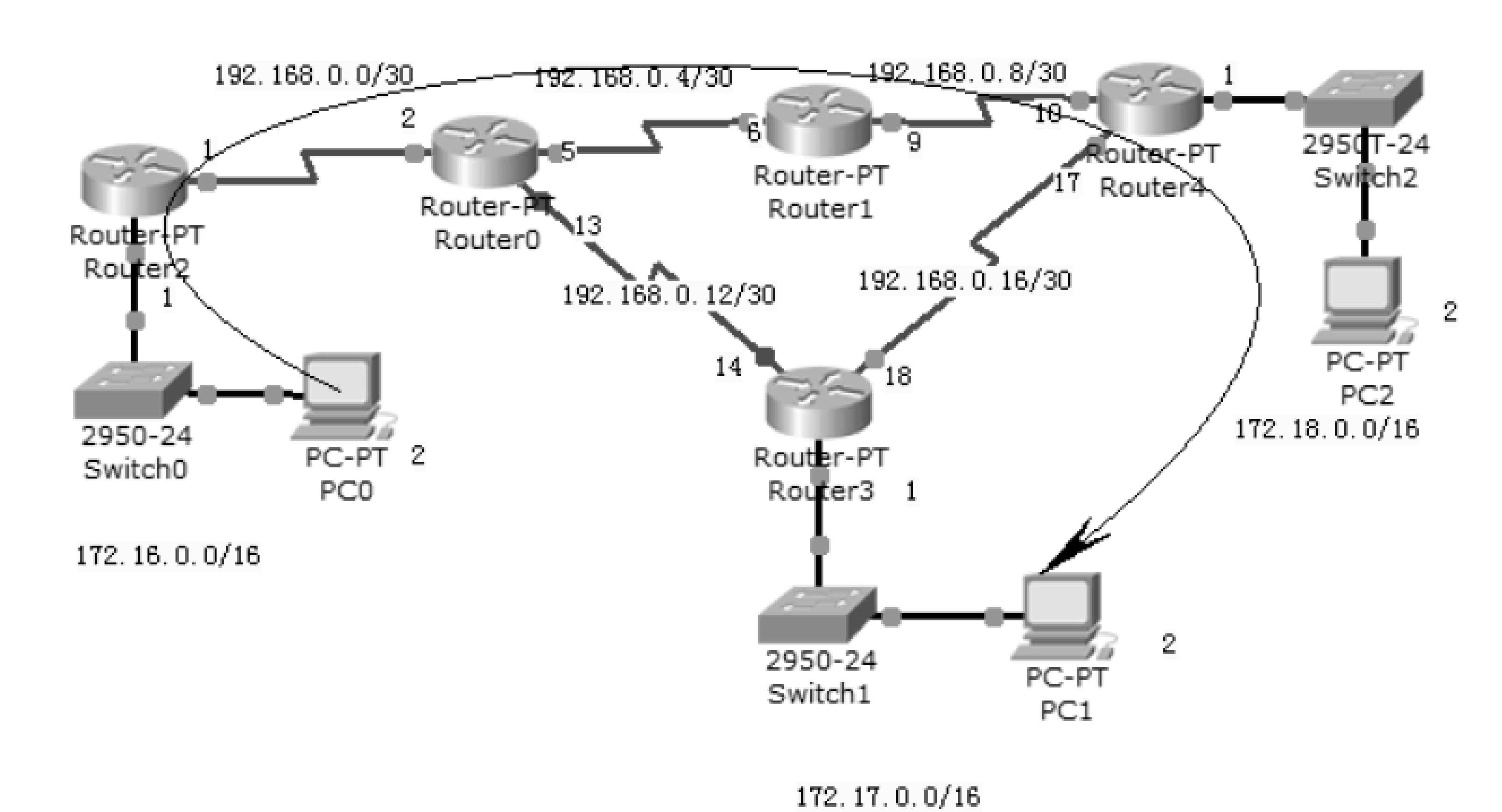
（2）在 Router3 上，关闭一个串行接口。

```
Router (config) #interface serial 2/0
Router (config-if) #shutdown
```

（3）在 PC0 上，再次跟踪到 PC1 的数据包路径。

```
PC>tracert 172.17.0.2
Tracing route to 172.17.0.2 over a maximum of 30 hops:
  1   9 ms      6 ms     7 ms     172.16.0.1
  2   15 ms     11 ms    13 ms    192.168.0.2
  3   14 ms     14 ms    16 ms    192.168.0.6
  4   19 ms     22 ms    15 ms    192.168.0.10
  5   26 ms     25 ms    29 ms    192.168.0.18
  6   29 ms     30 ms    36 ms    172.17.0.2
Trace complete.
```

你可以看到数据包途径 Router2→Router0→Router1→Router4→Router3，收敛速度很快，如图 6-18 所示。

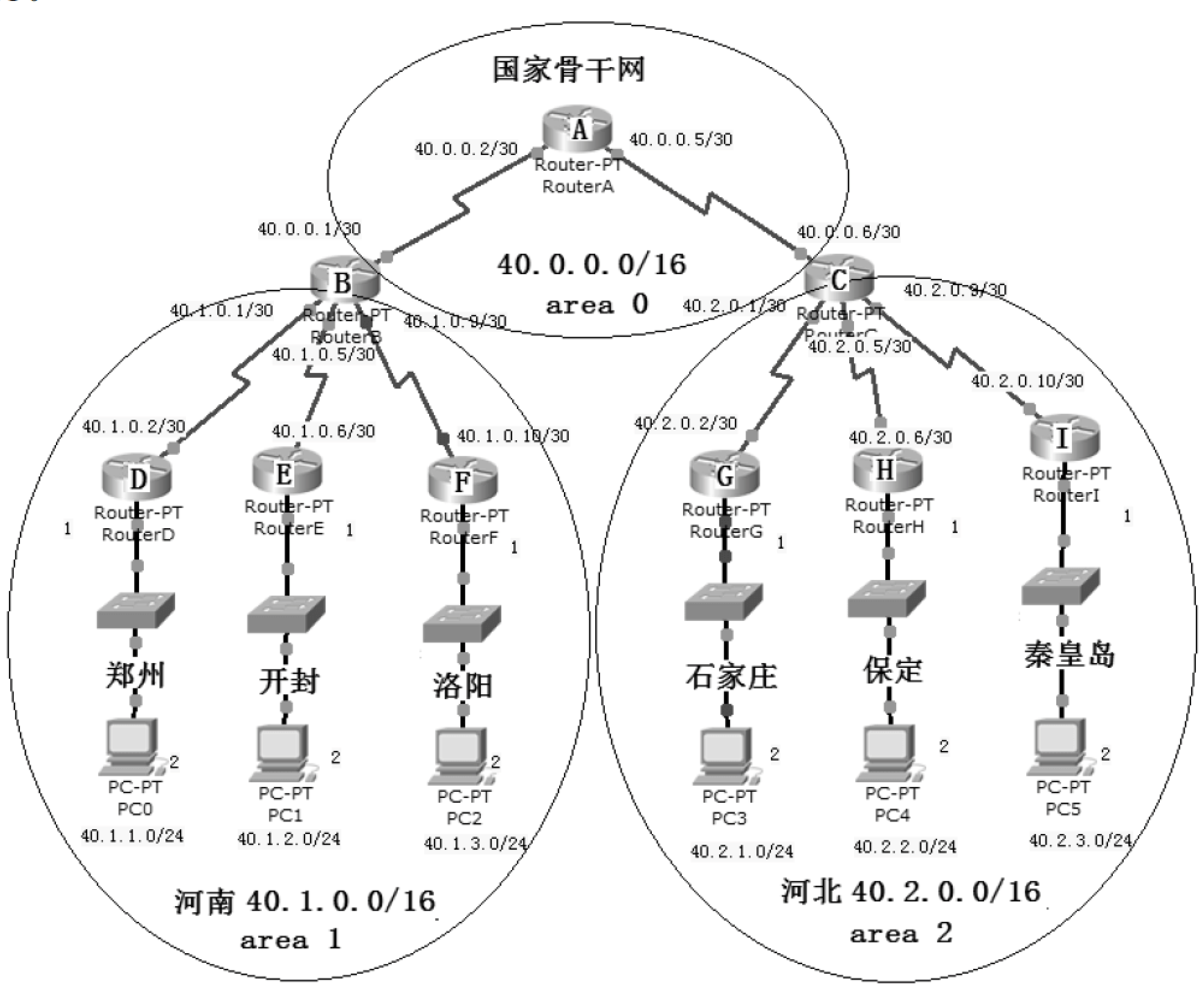


▲图 6-18　OSPF 选择的路径

6.4.8 OSPF 多区域

打开随书光盘中第 6 章练习“04　OSPF 多区域.pkt”，网络拓扑和 IP 地址规划如图 6-19 所示。配置 OSPF 协议支持多区域，国家骨干网是 OSPF 的 area 0 区域，使用 40.0.0.0/16 子网，河南省使用 40.1.0.0/16 子网，配置为 OSPF 的 area 1，河北省使用 40.2.0.0/16 子网，配置为 OSPF 的 area 2。

网络中的路由和计算机按照图示已经配置好了 IP 地址，你需要在这些路由器上配置 OSPF。



▲图 6-19　OSPF 多区域

配置步骤如下。

（1）在 RouterA 上，启用和配置 OSPF 协议。

```
RouterA>en
RouterA#config t
RouterA (config) #router ospf 1
RouterA (config-router) #network 40.0.0.0 0.0.0.255 area 0
```

（2）在 RouterB 上，启用和配置 OSPF 协议。

```
RouterB (config) #router ospf 1
RouterB (config-router) #network 40.0.0.0 0.0.255.255 area 0
```

```
RouterB (config-router) #network 40.1.0.0 0.0.255.255 area 1
```

(3) 在 RouterC 上，启用和配置 OSPF 协议。

```
RouterC (config) #router ospf 1
RouterC (config-router) #network 40.0.0.0 0.0.255.255 area 0
RouterC (config-router) #network 40.2.0.0 0.0.255.255 area 2
```

(4) 在 RouterD、RouterE 和 RouterF 上，启用和配置 OSPF 协议。

```
RouterD (config) #router ospf 1
RouterD (config-router) #network 40.1.0.0 0.0.255.255 area 1
```

(5) 在 RouterG、RouterH 和 RouterI 上，启用和配置 OSPF 协议。

```
RouterG (config) #router ospf 1
RouterG (config-router) #network 40.2.0.0 0.0.255.255 area 2
```

(6) 在 RouterA 上查看路由表。

可以看到 area 1 和 area 2 在区域边界路由器上没有汇总，在 area 0 中可以看到 area 1 和 area 2 内部各个网段的路由。在边界路由器手动配置可以将 area 1 网络中的网段汇总为一条路由到 area 0。Packet Tracer 不支持在 OSPF 的区域边界汇总，所以下面的实验将会使用 Dynamips 软件演示 OSPF 将 area 1 的网络汇总成一条通告给 area 0 的路由器。

```
RouterA#show ip route
Gateway of last resort is not set
    40.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C       40.0.0.0/30 is directly connected, Serial2/0
C       40.0.0.4/30 is directly connected, Serial3/0
O IA    40.1.0.0/30 [110/1562] via 40.0.0.1, 00:36:03, Serial2/0
O IA    40.1.0.4/30 [110/1562] via 40.0.0.1, 00:36:03, Serial2/0
O IA    40.1.0.8/30 [110/1562] via 40.0.0.1, 00:36:03, Serial2/0
O IA    40.1.1.0/24 [110/1563] via 40.0.0.1, 00:17:58, Serial2/0
O IA    40.1.2.0/24 [110/1563] via 40.0.0.1, 00:16:27, Serial2/0
O IA    40.1.3.0/24 [110/1563] via 40.0.0.1, 00:02:06, Serial2/0
O IA    40.2.0.0/30 [110/1562] via 40.0.0.6, 00:08:20, Serial3/0
O IA    40.2.0.4/30 [110/1562] via 40.0.0.6, 00:08:20, Serial3/0
O IA    40.2.0.8/30 [110/1562] via 40.0.0.6, 00:08:20, Serial3/0
O IA    40.2.1.0/24 [110/1563] via 40.0.0.6, 00:08:20, Serial3/0
O IA    40.2.2.0/24 [110/1563] via 40.0.0.6, 00:08:20, Serial3/0
O IA    40.2.3.0/24 [110/1563] via 40.0.0.6, 00:08:20, Serial3/0
```

IA 代表 OSPF 到其他区域网络的路由，中括号中的 110 代表管理距离，后面的值是度量值。

```
RouterA#show ip ospf interface      --显示接口的 OSPF 配置信息和状态
RouterB#show ip ospf database       --显示路由的链路状态数据库
```

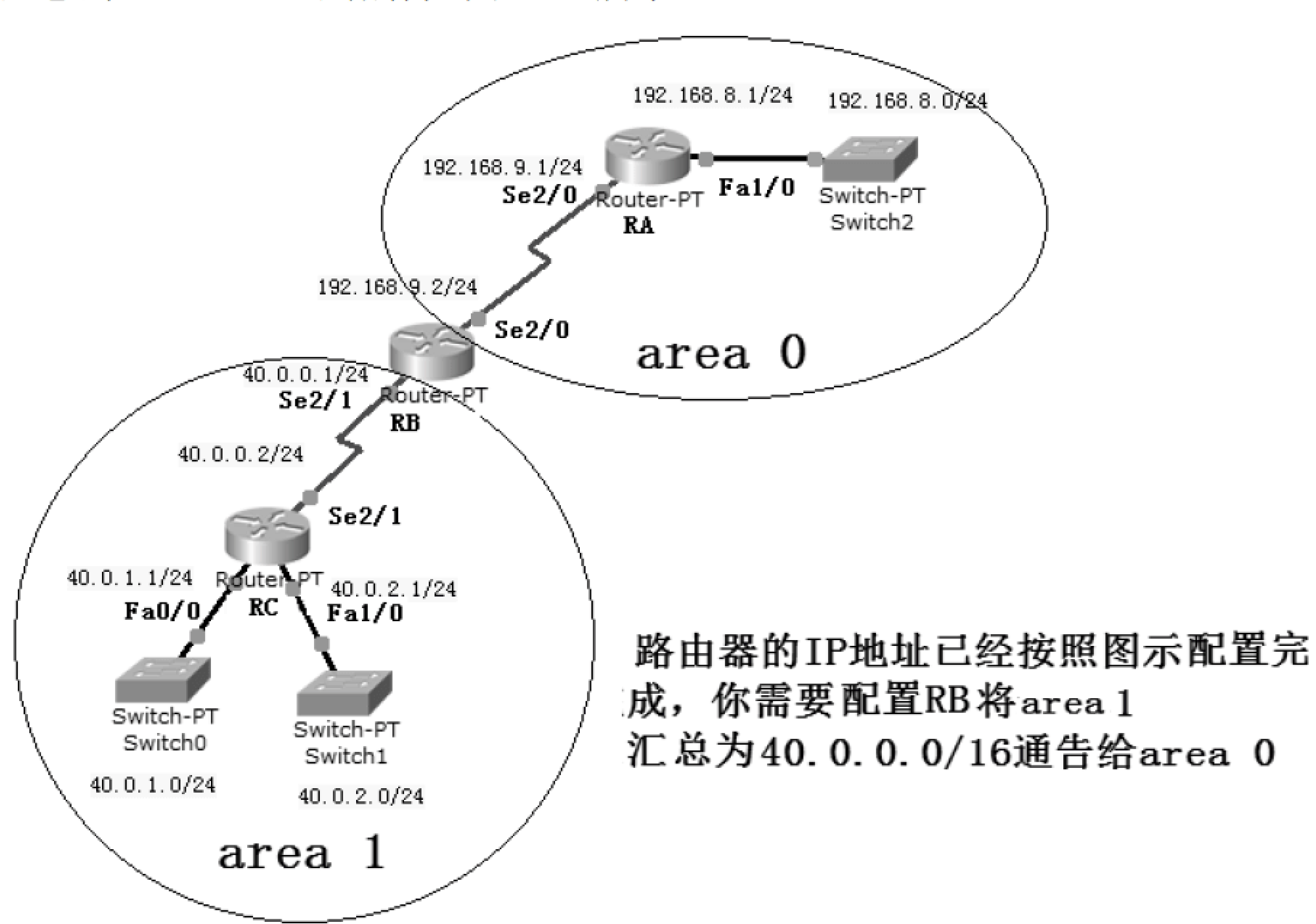
```
RouterA#debug ip ospf events          --显示 OSPF 事件，比如 Hello 包的收发
```

以上实验 area 1 和 area 2 可以汇总为一条路由通告给 area 0，但是 Packet Tracer 软件模拟的路由器不支持区域汇总。下面的实验在 Dynamips 软件实现 OSPF 区域汇总。

6.4.9 OSPF 路由汇总

本节配置 OSPF 在区域边界进行路由汇总。

以下的实验将会使用本书第 4 章的 Dynamips 软件搭建的实验环境，演示 OSPF 将 area 1 的网络汇总到 area 0，网络拓扑如图 6-20 所示。



▲图 6-20 网络拓扑

按照图 6-20 所示地址配置网络中路由器 IP 地址，你需要配置路由器启用 OSPF，并将相应的接口指定到不同的 OSPF 区域，然后将 area 1 的网络汇总成一条通告给 area 0。

操作步骤如下。

（1）在 RouterA 上，进入全局配置模式配置 OSPF。

```
RA (config) #router ospf 1
RA (config-router) #network 192.168.8.0 0.0.0.255 area 0
RA (config-router) #network 192.168.9.0 0.0.0.255 area 0
```

（2）在 RouterB 上，进入全局配置模式配置 OSPF。

```
RB (config) #router ospf 1
RB (config-router) #network 192.168.9.0 0.0.0.255 area 0
RB (config-router) #network 40.0.0.0 0.0.0.255 area 1
```

（3）在 RouterC 上，进入全局配置模式配置 OSPF。

```
RC (config) #router ospf 1
RC (config-router) #network 40.0.0.0 0.0.255.255 area 1
```

（4）在 RouterA 上，查看路由表，可以看到 OSPF 区域的 3 个子网，子网掩码是 24。

```
RA#show ip route
Gateway of last resort is not set

C    192.168.8.0/24 is directly connected, FastEthernet0/0
C    192.168.9.0/24 is directly connected, Serial1/0
     40.0.0.0/24 is subnetted, 3 subnets      子网掩码是24，3个子网
O IA    40.0.0.0 [110/128] via 192.168.9.2, 00:00:00, Serial1/0
O IA    40.0.1.0 [110/129] via 192.168.9.2, 00:00:00, Serial1/0
O IA    40.0.2.0 [110/129] via 192.168.9.2, 00:00:00, Serial1/0
```

（5）在 RB 上进行汇总，将汇总为 40.0.0.0/16。

```
RB (config) #router ospf 1
RB (config-router) #area 1 range 40.0.0.0 255.255.0.0
```

（6）在 RouterA 上，查看 area 1 汇总过来的路由表，注意观察子网掩码为 16。

```
RA#show ip route
Gateway of last resort is not set candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
C    192.168.8.0/24 is directly connected, FastEthernet0/0
C    192.168.9.0/24 is directly connected, Serial1/0
     40.0.0.0/16 is subnetted, 1 subnets      子网掩码是16，1个子网
O IA    40.0.0.0 [110/128] via 192.168.9.2, 00:00:26, Serial1/0
```

6.5 RIP、EIGRP 和 OSPF 协议的对比

以上讲述了 RIP、EIGRP 和 OSPF 的配置方法。现在对这几种协议进行对比。

6.5.1 路由协议的类型

路由协议分以下几种类型。

- 距离矢量协议：典型代表就是 RIP，其特点就是周期性广播或多播，将自己的路由表通告给其他路由器。
- 链路状态协议：典型代表就是 OSPF，其特点就是周期性使用 Hello 包维护邻居信息、触发式更新链路状态、使用链路状态数据库计算路由表。
- 混合型协议：典型代表就是 EIGRP，为什么说它是混合的呢？因为使用 Hello 包维护邻居信息、触发式更新，这些特性像链路状态的部分特性，但是它又直接通告路由表到其他路由器，此特性是距离矢量的特性，因此称 EIGRP 为混合型。

这三种协议的功能对比如表 6-1 所示。

表 6-1　RIP、EIGRP 和 OSPF 协议功能对比

特性	RIPv1	RIPv2	EIGRP	OSPF
协议类型	距离矢量	距离矢量	混合	链路状态
无类支持	否	是	是	是
VLSM 支持	否	是	是	是
自动汇总	是	是	是	否
手动汇总	否	否	是	是
不连续子网支持	否	是	是	是
路由传播	周期性广播	周期性组播	触发式	触发式更新
度量值	跳数	跳数	带宽和延迟	带宽
跳数限制	15	15	最大 255	无
汇聚	慢	慢	最快	快
分层网络	否	否	自制系统	分区域
更新	直接更新路由表	直接更新路由表	触发式更新	事件触发
路由计算	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra

6.5.2　路由协议的优先级

如果网络中的路由器运行了多个路由协议，比如 EIGRP 和 RIP，这两个协议都学到了到某个网段的路由。到底以哪一条为准呢？这就需要用动态路由协议的管理距离（AD）来确定。

管理距离是用来衡量接收来自相邻路由器上路由选择信息的可信度的。一个管理距离是一个从 0～255 的整数值，0 是最可信赖的，而 255 则意味着不会有业务量通过该路由。

如果一台路由器接收到两个对同一远程网络的更新内容，路由器首先要检查的是 AD。如果一个被通告的路由比另一个具有较低的 AD 值，则那个带有较低 AD 值的路由将会被放置在路由表中。

如果两个被通告的到同一网络的路由具有相同的 AD 值，则路由协议的度量值（如跳数或链路的带宽值）将被用作寻找到达远程网络最佳路径的依据。被通告的带有最低度量值的路由将被放置在路由表中。然而，如果两个被通告的路由具有相同的 AD 及相同的度量值，那么路由选择协议将会对这一远程网络使用负载均衡（即它所发送的数据包会平分到每个链路上）。

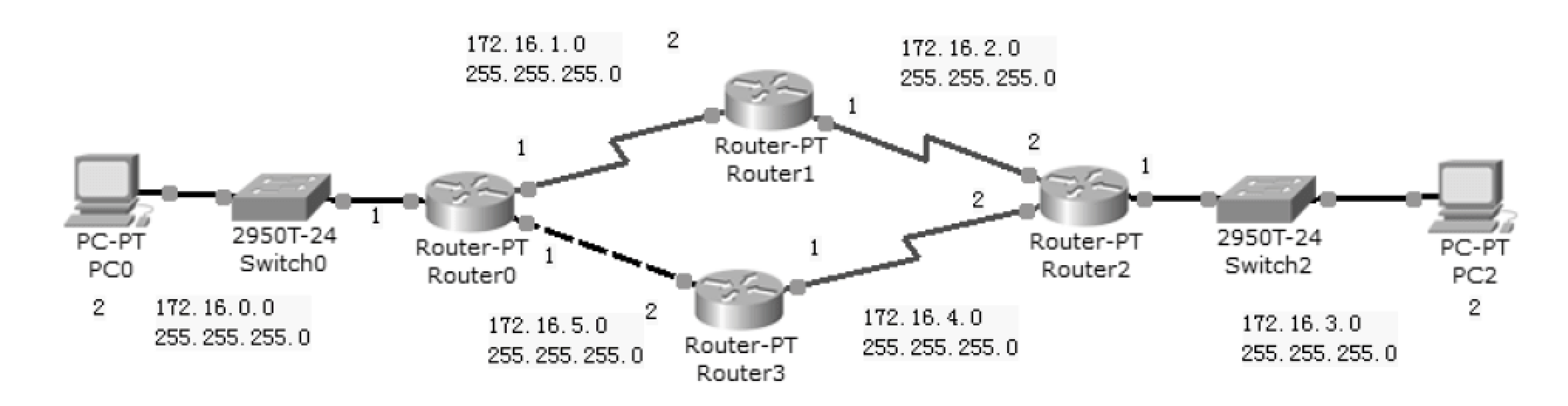
表 6-2 列出了默认的管理距离。

表 6-2 默认管理距离

路由源	默认 AD
连接接口	0
静态路由	1
EIGRP	90
OSPF	110
RIP	120
External EIGRP	170
未知	255（这个路由绝不会被使用）

6.5.3 验证路由协议的优先级

打开随书光盘中第 6 章练习“05 验证路由协议优先级.pkt”，如图 6-21 所示。网络中的路由器和计算机的 IP 地址已经配置。



▲图 6-21 网络拓扑

你需要先配置路由器使用 RIP 协议，再配置路由器使用 OSPF，然后配置路由器使用 EIGRP 协议，最后添加静态路由。查看路由器的路由表，验证这些动态路由协议的优先级。

操作步骤如下。

（1）配置网络中的路由器使用 RIP 协议，在所有的路由器上运行以下命令。

```
Router (config) #router rip
Router (config-router) #network 172.16.0.0
```

（2）在 Router0 上查看路由表。

```
Router0#show ip route
        172.16.0.0/24 is subnetted, 6 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
C       172.16.1.0 is directly connected, Serial2/0
R       172.16.2.0 [120/1] via 172.16.1.2, 00:00:22, Serial2/0
R       172.16.3.0 [120/2] via 172.16.5.2, 00:00:04, FastEthernet1/0
                   [120/2] via 172.16.1.2, 00:00:22, Serial2/0
```

```
R       172.16.4.0 [120/1] via 172.16.5.2, 00:00:04, FastEthernet1/0
C       172.16.5.0 is directly connected, FastEthernet1/0
```

可以看到到达 172.16.3.0/24 网段有两条等价路径，管理距离为 120，度量值为 2，也就是 2 跳。

（3）配置网络中的路由器使用 OSPF 协议，使这些路由器工作在 OSPF 区域 0，在所有的路由器上运行以下命令。

```
Router (config) #router ospf 1
Router (config-router) #network 172.16.0.0 0.0.255.255 area 0
```

（4）在 Router0 上查看路由表。

```
Router0#show ip route
        172.16.0.0/24 is subnetted, 6 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
C       172.16.1.0 is directly connected, Serial2/0
O       172.16.2.0 [110/1562] via 172.16.1.2, 00:02:31, Serial2/0
O       172.16.3.0 [110/783] via 172.16.5.2, 00:01:51, FastEthernet1/0
O       172.16.4.0 [110/782] via 172.16.5.2, 00:01:51, FastEthernet1/0
C       172.16.5.0 is directly connected, FastEthernet1/0
```

可以看到通过 RIP 学到的路由已经不出现，只显示通过 OSPF 学到的路由。管理距离为 110，到 172.16.3.0/24 网络的路由，度量值为 783，是一条最佳路径。

（5）配置网络中的路由器使用 EIGRP 协议，自制系统编号为 10，在所有的路由器上运行以下命令。

```
Router  (config) #router eigrp 10
Router  (config-router) #network 172.16.0.0
```

（6）在 Router0 上查看路由。

```
Router0#show ip route
Gateway of last resort is not set
        172.16.0.0/24 is subnetted, 6 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
C       172.16.1.0 is directly connected, Serial2/0
D       172.16.2.0 [90/21024000] via 172.16.1.2, 00:00:46, Serial2/0
D       172.16.3.0 [90/20517120] via 172.16.5.2, 00:00:14, FastEthernet1/0
D       172.16.4.0 [90/20514560] via 172.16.5.2, 00:00:14, FastEthernet1/0
C       172.16.5.0 is directly connected, FastEthernet1/0
```

可以看到通过 OSPF 和 RIP 协议学到的路由不再显示，只出现通过 EIGRP 学到的路由表，因为 EIGRP 协议的管理距离为 90，比 OSPF 协议和 RIP 协议的管理距离小，达到 172.16.3.0/24 网段的度量值为 20517120。

（7）在 Router2 上禁用 EIGRP。

```
Router2 (config) #no router eigrp 10
```

（8）在 Router0 上添加到 172.16.2.0/24 网段的路由。

```
Router0 (config) #ip route 172.16.2.0 255.255.255.0 172.16.1.2 ?
  <1-255>  Distance metric for this route
  <cr>
Router0 (config) # ip route 172.16.2.0 255.255.255.0 172.16.1.2
--使用默认的 AD
默认管理距离为 1，可改为其他的值
```

（9）在 Router0 上查看路由表。

```
Router0#show ip route
Gateway of last resort is not set
       172.16.0.0/24 is subnetted, 6 subnets
C      172.16.0.0 is directly connected, FastEthernet0/0
C      172.16.1.0 is directly connected, Serial2/0
S      172.16.2.0 [1/0] via 172.16.1.2
O      172.16.3.0 [110/783] via 172.16.5.2, 00:03:23, FastEthernet1/0
D      172.16.4.0 [90/20514560] via 172.16.5.2, 00:03:23, FastEthernet1/0
C      172.16.5.0 is directly connected, FastEthernet1/0
```

到 172.16.2.0/24 网段的路由是静态路由，管理距离为 1，因此通过 RIP、OSPF 和 EIGRP 学到的到该网段的路由都不出现。

由于在 Router2 上禁用了 EIGRP，到 172.16.3.0/24 网段的路由是通过 OSPF 学到的。可见路由器上的路由表可以通过多个 IP 协议和静态路由共同构造。

（10）在 Router0 上查看路由器运行的所有的动态路由协议。

```
Router#show ip protocols
```

通过本实验，可以得到以下结论。

网络中的路由器可以同时运行多种动态路由协议（通常不会配置路由器同时运行多种动态路由协议，因为这样做比较消耗路由器的 CPU 和网络带宽）和静态路由，路由器可以通过多个动态路由协议学到到某个网段的路由，管理距离值较小的协议学到的路由出现在路由表中。

6.6 路由再发布

路由器上的静态路由通常不会被动态路由协议通告出去。如果你需要将某个路由器的静态路由通过动态路由协议通告出去，就需要将静态路由发布到动态路由。

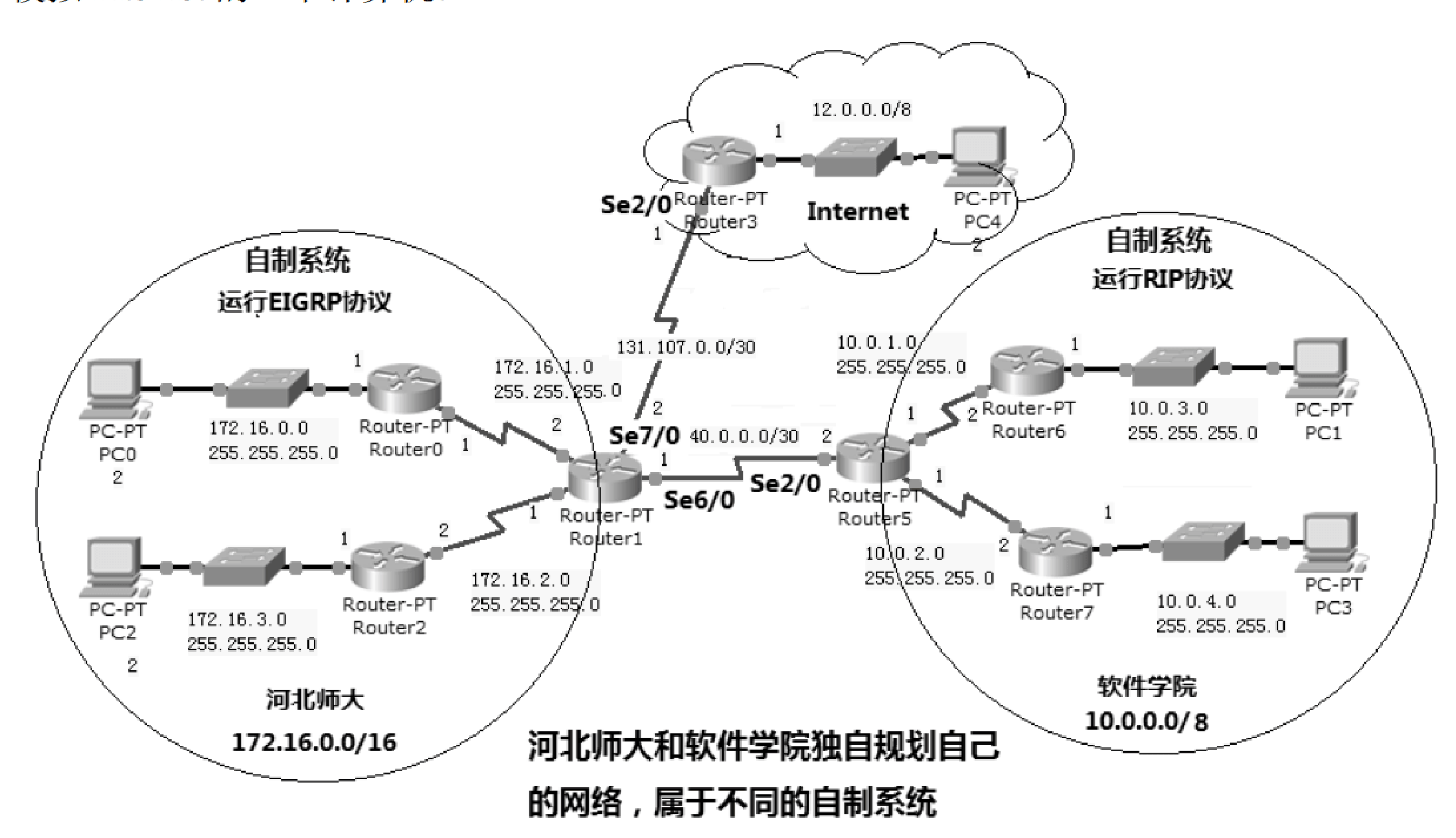
不同的动态路由协议之间需要交换路由表，也需要进行路由再发布。

下面就举两个例子演示将静态路由发布到动态路由，以及不同的动态路由协议之间进行

路由再发布。

6.6.1 将静态路由发布到动态路由

打开随书光盘中第 6 章练习“06 将静态路由发布到动态路由.pkt”，如图 6-22 所示，河北师大和软件学院有各自独立的网络，有独立的 IT 部门管理自己的网络。Router1 是访问 Internet 的出口。河北师大的内部网络配置 EIGRP 协议，可以认为是一个自制系统。软件学院的内部网络配置 RIP 协议，可以认为是一个自制系统。Router3 模拟 Internet 的路由器，PC4 模拟 Internet 的一个计算机。



▲图 6-22 静态路由再发布实验的网络拓扑

1. 实验环境

网络中的计算机和路由器已经按照图 6-22 所示的地址配置完成。

Router3 已经添加了到 172.16.0.0/16 和 10.0.0.0/8 网段的路由。

Router0、Router1 和 Router2 配置了 EIGRP 协议。

Router5、Router6 和 Router7 配置了 RIP 协议。

2. 实验要求

Router1 是河北师大的边界路由器，需要在 Router1 上添加到 10.0.0.0/16 网段的静态路由和指向 Internet 的默认路由，然后让 Router1 使用 EIGRP 将这两条静态路由通告给 Router0 和 Router2。

Router5 是软件学院的边界路由器，需要在 Router5 上添加一条默认路由，然后让 Router5 使用 RIP 将该默认路由通告给 Router6 和 Router7。

3. 操作步骤

（1）在 Router1 上添加静态路由和查看路由表。

```
Router1 (config) #ip route 10.0.0.0 255.0.0.0 Serial 6/0  --指向接口的静态路由
Router1 (config) #ip route 0.0.0.0 0.0.0.0 Serial 7/0     --指向接口的静态路由
```

指向一个接口的静态路由应该只在点到点链路接口上使用。因为在其他接口上，路由器将不知道要发送信息去的具体地址。在点到点接口上，信息将只被发送到网络上的对端设备。这样添加的路由管理距离是 0，相当于该路由器直连这个网段，因此该网段才能通过动态路由协议通告出去。在这里绝对不能写下一跳的 IP 地址。

```
Router1#show ip route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S     10.0.0.0/8 is directly connected, Serial6/0 --该默认路由，相当于直连网络
       40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D      40.0.0.0/8 is a summary, 00:47:33, Null0
C      40.0.0.0/30 is directly connected, Serial6/0
       131.107.0.0/30 is subnetted, 1 subnets
C      131.107.0.0 is directly connected, Serial7/0
       172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
D      172.16.0.0/16 is a summary, 00:47:33, Null0
D      172.16.0.0/24 [90/20514560] via 172.16.1.1, 00:47:33, Serial3/0
C      172.16.1.0/24 is directly connected, Serial3/0
C      172.16.2.0/24 is directly connected, Serial2/0
D      172.16.3.0/24 [90/20514560] via 172.16.2.2, 00:47:33, Serial2/0
S*    0.0.0.0/0 is directly connected, Serial7/0  --该默认路由，相当于直连网络
```

（2）在 Route1 上修改 EIGRP 配置，将到达 10.0.0.0 这个 A 类网络的路由和默认路由通告出去。

```
Router1 (config) #router eigrp 10
Router1 (config-router) #network 10.0.0.0
Router1 (config-router) #network 0.0.0.0
```

（3）在 Router5 上添加静态路由和修改 RIP 将默认路由通告出去。

```
Router5 (config) #ip route 0.0.0.0 0.0.0.0 Serial 2/0
Router5 (config) #router rip
Router5 (config-router) #network 0.0.0.0
```

（4）在 Router0 上查看路由表。

```
Router0#show ip route
Gateway of last resort is 172.16.1.2 to network 0.0.0.0
D   10.0.0.0/8 [90/21024000] via 172.16.1.2, 00:01:50, Serial2/0
                                                   --到软件学院的路由
```

```
D    40.0.0.0/8 [90/21024000] via 172.16.1.2, 00:52:00, Serial2/0
D    131.107.0.0/16 [90/21024000] via 172.16.1.2, 00:01:50, Serial2/0
     172.16.0.0/24 is subnetted, 4 subnets
C    172.16.0.0 is directly connected, FastEthernet0/0
C    172.16.1.0 is directly connected, Serial2/0
D    172.16.2.0 [90/21024000] via 172.16.1.2, 00:52:00, Serial2/0
D    172.16.3.0 [90/21026560] via 172.16.1.2, 00:52:00, Serial2/0
D*   0.0.0.0/0 [90/21024000] via 172.16.1.2, 00:01:50, Serial2/0
                                                  --到 Internet 的默认路由
```

河北师大的内部路由器通过 EIGRP 学习到了边界路由器 Router1 通告的到 Internet 的默认路由和到软件学院的静态路由。

（5）在 Router6 上查看路由表。

```
Router6#show ip route
Gateway of last resort is 10.0.1.1 to network 0.0.0.0
     10.0.0.0/24 is subnetted, 4 subnets
C    10.0.1.0 is directly connected, Serial2/0
R    10.0.2.0 [120/1] via 10.0.1.1, 00:00:26, Serial2/0
C    10.0.3.0 is directly connected, FastEthernet0/0
R    10.0.4.0 [120/2] via 10.0.1.1, 00:00:26, Serial2/0
R    40.0.0.0/8 [120/1] via 10.0.1.1, 00:00:26, Serial2/0
R*   0.0.0.0/0 [120/1] via 10.0.1.1, 00:00:26, Serial2/0  --学到的默认路由
```

软件学院的内部路由器通过 RIP 协议学习到了边界路由器 Router5 通告的默认路由。

（6）在 PC0 上跟踪到达 PC1 的数据包路径。

```
PC>tracert 10.0.3.2
```

（7）在 PC0 上跟踪到达 PC4 的数据包。

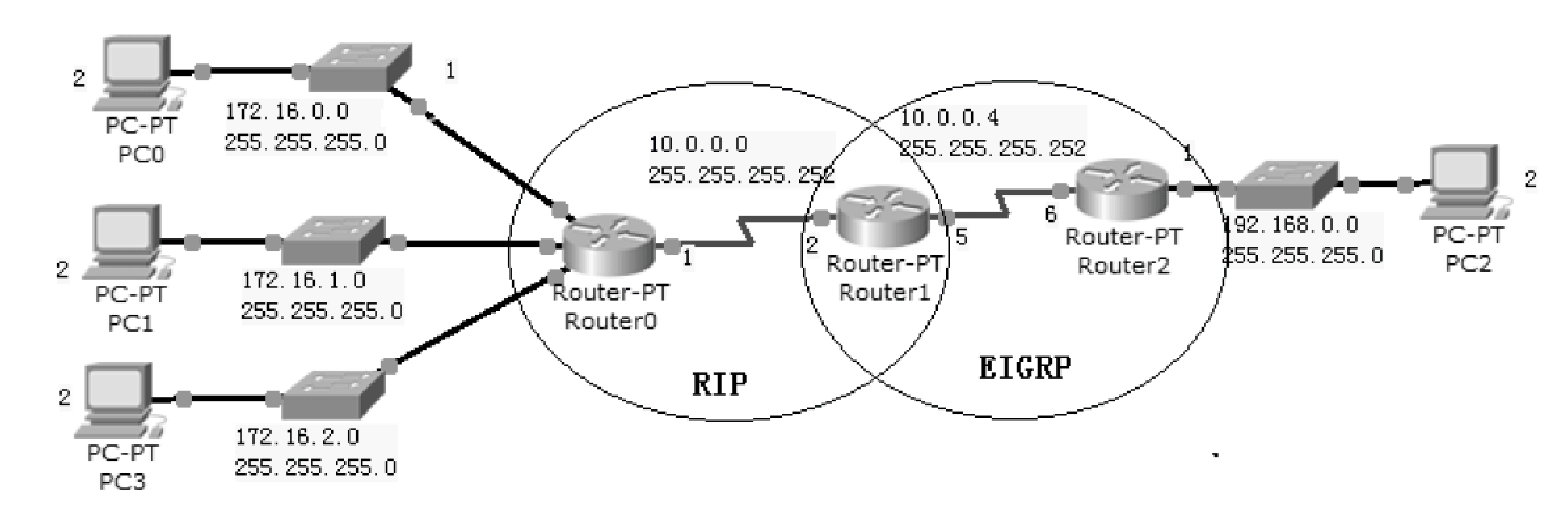
```
PC>tracert 12.0.0.2
```

6.6.2 RIP 和 EIGRP 路由再发布

不同的动态路由协议之间需要交换路由表，也需要进行路由再发布。

打开随书光盘中第 6 章练习“07 RIP 和 EIGRP 路由再发布.pkt”，网络拓扑如图 6-23 所示。网络中的路由器和计算机已经按照图示的地址配置完成。Router0 和 Router1 运行了 RIPv2，并且关闭了自动汇总，Router1 和 Router2 运行了 EIGRP 协议。

你需要配置 Router1 将 EIGRP 协议学到的路由通过 RIP 协议通告给 Router0；配置 Router1 将 RIPv2 学到的路由通过 EIGRP 协议通告给 Router2。



▲图 6-23　RIP 和 EIGRP 路由再发布的网络拓扑

操作步骤如下。

（1）在 Router1 上运行 show ip route 命令查看路由表。

```
Router1#show ip route
Gateway of last resort is not set
        10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, Serial3/0
C       10.0.0.4 is directly connected, Serial2/0
        172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R       172.16.0.0/24 [120/1] via 10.0.0.1, 00:00:26, Serial3/0
R       172.16.1.0/24 [120/1] via 10.0.0.1, 00:00:26, Serial3/0
R       172.16.2.0/24 [120/1] via 10.0.0.1, 00:00:26, Serial3/0
D       192.168.0.0/24 [90/20514560] via 10.0.0.6, 00:35:10, Serial2/0
```

可以看到在 Router1 上的路由表中包括了通过 RIP 协议学到的路由和通过 EIGRP 协议学到的路由。

（2）在 Router0 上查看路由表。

```
Router0#show ip route
Gateway of last resort is not set
        10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, Serial2/0
R       10.0.0.4 [120/1] via 10.0.0.2, 00:00:14, Serial2/0
        172.16.0.0/24 is subnetted, 3 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0
C       172.16.1.0 is directly connected, FastEthernet1/0
C       172.16.2.0 is directly connected, FastEthernet6/0
```

可以看到 Router1 没有将其通过 EIGRP 学到的路由通过 RIP 协议通告给 Router0。

（3）在 Router2 上查看路由表。

同样可以看到 Router1 没有将其通过 RIP 学到的路由通过 EIGRP 协议通告给 Router2。

（4）在 Router1 上配置将 EIGRP 发布到 RIP。

```
Router1#config t
Router1 (config) #router rip
Router1 (config-router) #redistribute eigrp 10 metric ?
  <0-16>       Default metric
  transparent  Transparently redistribute metric
Router1 (config-router) #redistribute eigrp 10 metric 3
```

最后一条命令将 EIGRP 协议学到的路由度量值转化为 RIP 协议的度量值 3。

（5）在 Router1 上配置将 RIP 发布到 EIGRP。

```
Router1 (config) #router eigrp 10
Router1 (config-router) #redistribute rip metric 10000 100 255 1 1500
```

最后一条命令是将 RIP 学到的路由度量值转化为 EIGRP 的度量值。其中：

10000：是带宽，单位是 kb/s；

100：是延迟，单位是 10us；

255：是可靠性，值可以是 0～255，255 是 100%可靠；

1：是负载，值可以是 1～255，255 是 100%负载，即网络将要堵塞；

1500：是最大传输单元（MTU），单位为 8 比特字节。

（6）在 Router0 上查看路由表。

```
Router0#show ip route
Gateway of last resort is not set
     10.0.0.0/30 is subnetted, 2 subnets
C    10.0.0.0 is directly connected, Serial2/0
R    10.0.0.4 [120/1] via 10.0.0.2, 00:00:04, Serial2/0
     172.16.0.0/24 is subnetted, 3 subnets
C    172.16.0.0 is directly connected, FastEthernet0/0
C    172.16.1.0 is directly connected, FastEthernet1/0
C    172.16.2.0 is directly connected, FastEthernet6/0
R    192.168.0.0/24 [120/3] via 10.0.0.2, 00:12:34, Serial2/0
                                                    --学到了再发布的路由
```

（7）在 Router2 上查看路由表。

```
Router2#show ip route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D    10.0.0.0/8 is a summary, 01:04:04, Null0
D    10.0.0.0/30 [90/21024000] via 10.0.0.5, 01:04:04, Serial3/0
C    10.0.0.4/30 is directly connected, Serial3/0
     172.16.0.0/24 is subnetted, 3 subnets
D EX    172.16.0.0 [170/20537600] via 10.0.0.5, 00:07:39, Serial3/0
```

```
                                                       --再发布的路由
D EX   172.16.1.0 [170/20537600] via 10.0.0.5, 00:07:39, Serial3/0
                                                       --再发布的路由
D EX   172.16.2.0 [170/20537600] via 10.0.0.5, 00:07:39, Serial3/0
                                                       --再发布的路由
C      192.168.0.0/24 is directly connected, FastEthernet0/0
```

可以看到 D EX 开头的路由是 EIGRP 的外部路由，也就是 RIP 发布到 EIGRP 的路由，管理距离是 170。

（8）在 PC0 上 ping PC2，测试网络是否通。

```
PC>ping 192.168.0.2
```

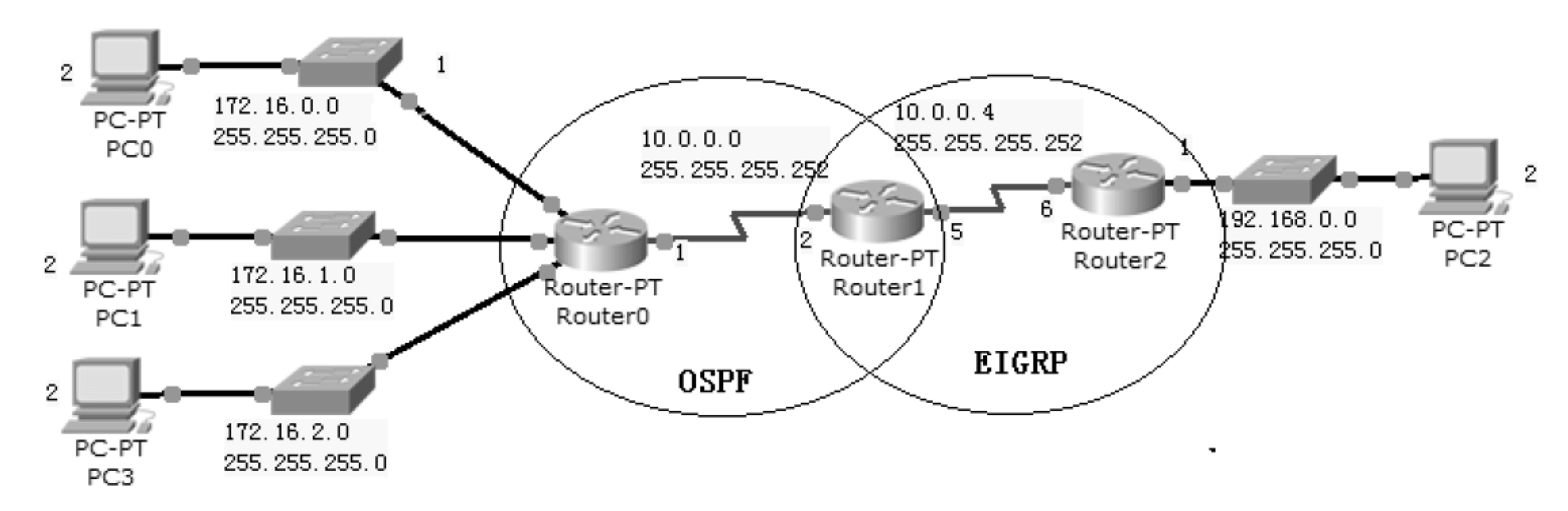
（9）在 Router1 上取消再发布。

```
Router1 (config) #router eigrp 10
Router1 (config-router) #no redistribute rip          --取消 EIGRP 到 RIP 的发布
Router1 (config) #router rip
Router1 (config-router) #no redistribute eigrp 10  --取消 RIP 到 EIGRP 的发布
```

6.6.3 OSPF 和 EIGRP 路由再发布

打开随书光盘中第 6 章练习“07　OSPF 和 EIGRP 路由再发布.pkt”，网络拓扑如图 6-24 所示，网络中的路由器和计算机已经按照图示的地址配置完成。Router0 和 Router1 运行了 OSPF，都工作在 area 0，Router1 和 Router2 运行了 EIGRP 协议。

你需要配置 Router1 将 EIGRP 协议学到的路由通过 OSPF 协议通告给 Router0；配置 Router1 将 OSPF 学到的路由通过 EIGRP 协议通告给 Router2。



▲图 6-24　OSPF 和 EIGRP 路由再发布的网络拓扑

操作步骤如下。

（1）在 Router0、Router1 和 Router2 上查看路由表，运行 show ip route 命令，注意观察路由表，Router1 路由表有到所有网络的路由。

（2）在 Router1 上配置将 EIGRP 发布到 OSPF。

```
Router1 (config) #router ospf 1
```

```
Router1 (config-router) #redistribute eigrp 10 metric 30 metric-type 1 subnets
```

以上命令将 EIGRP 10 学到的路由重新分配进入 OSPF 进程 1。命令的度量部分为每一条重新分配的路由分配度量值，度量值是 OSPF 代价值 30。重新分配使得 Router1 作为 OSPF 域的 ASBR。被重新分配的路由是作为外部路由进行通告的。命令 metric-type 部分指明了外部路由的类型为 E1。关键字 subnets 仅当 OSPF 发布路由时使用，它指明了重新分配的子网细节，如果没有它，仅重新分配主网地址。

（3）在 Router1 上配置将 OSPF 发布到 EIGRP。

```
Router1 (config) #router eigrp 10
Router1 (config-router) #redistribute ospf 1 metric 10000 100 255 1 1500
```

以上命令将 OSPF 协议学到的路由重新分配进入 EIGRP 10，并且指明 EIGRP 对应的度量值，依次为带宽、延迟、可靠性、负载和最大传输单元。

（4）在 Router0 上查看路由表。

```
Router0#show ip route
Gateway of last resort is not set
       10.0.0.0/30 is subnetted, 2 subnets
C      10.0.0.0 is directly connected, Serial2/0
O      10.0.0.4 [110/1562] via 10.0.0.2, 00:25:23, Serial2/0
       172.16.0.0/24 is subnetted, 3 subnets
C      172.16.0.0 is directly connected, FastEthernet0/0
C      172.16.1.0 is directly connected, FastEthernet1/0
C      172.16.2.0 is directly connected, FastEthernet6/0
O E1   192.168.0.0/24 [110/811] via 10.0.0.2, 00:03:04, Serial2/0
       --OSPF 外部路由
```

（5）在 Router2 上查看路由表。

```
Router2#show ip route
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D     10.0.0.0/8 is a summary, 04:13:01, Null0
D     10.0.0.0/30 [90/21024000] via 10.0.0.5, 04:13:01, Serial3/0
C     10.0.0.4/30 is directly connected, Serial3/0
      172.16.0.0/24 is subnetted, 3 subnets
D EX  172.16.0.0 [170/20537600] via 10.0.0.5, 00:48:00, Serial3/0
                                                  --EIGRP 外部路由
D EX  172.16.1.0 [170/20537600] via 10.0.0.5, 00:48:00, Serial3/0
                                                  --EIGRP 外部路由
D EX  172.16.2.0 [170/20537600] via 10.0.0.5, 00:48:00, Serial3/0
                                                   --EIGRP 外部路由
```

```
C     192.168.0.0/24 is directly connected, FastEthernet0/0
```

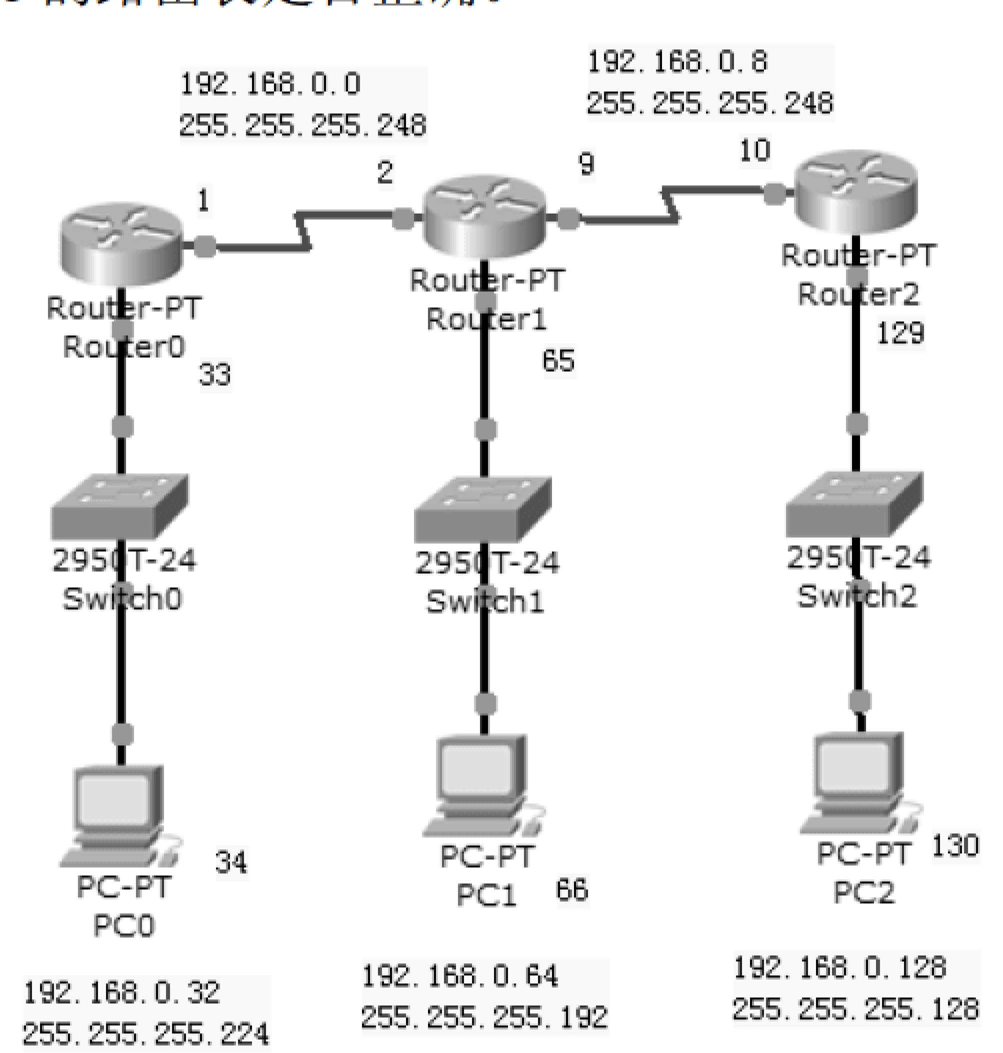
可以看到通过 EIGRP 学到的 OSPF 发布的路由，度量值为 170。

6.7 实验

6.7.1 实验 1：配置 RIPv2 支持变长子网

打开随书光盘中第 6 章“实验 1 配置 RIPv2 支持变长子网.pkt”。网络拓扑如图 6-25 所示，本实验用来验证 RIPv1 不支持变长子网，RIPv2 支持变长子网。

网络中的路由器和计算机都已经配置好了 IP 地址和子网掩码。你需要配置这些路由器使用 RIP 协议。查看 Router1 的路由表是否正确，然后将网络中的路由器的 RIP 协议更改为 RIPv2，再次查看 Router1 的路由表是否正确。



▲图 6-25　变长子网网络拓扑

操作步骤如下。

（1）在所有的路由器上运行以下命令启用 RIPv1。

```
Router (config) #router rip
Router (config-router) #network 192.168.0.0
```

（2）查看 Router1 的路由表。

```
Router#show ip route
Gateway of last resort is not set
       192.168.0.0/24 is variably subnetted, 3 subnets, 2 masks
C      192.168.0.0/29 is directly connected, Serial3/0
C      192.168.0.8/29 is directly connected, Serial2/0
C      192.168.0.64/26 is directly connected, FastEthernet0/0
```

可以看到根本就没有通过 RIP 学到到其他网段的路由表。

（3）在所有的路由器上运行以下命令，将 RIP 更改为 RIPv2。

```
Router (config) #router rip
Router (config-router) #version 2
```

（4）再次查看 Router1 上的路由表。

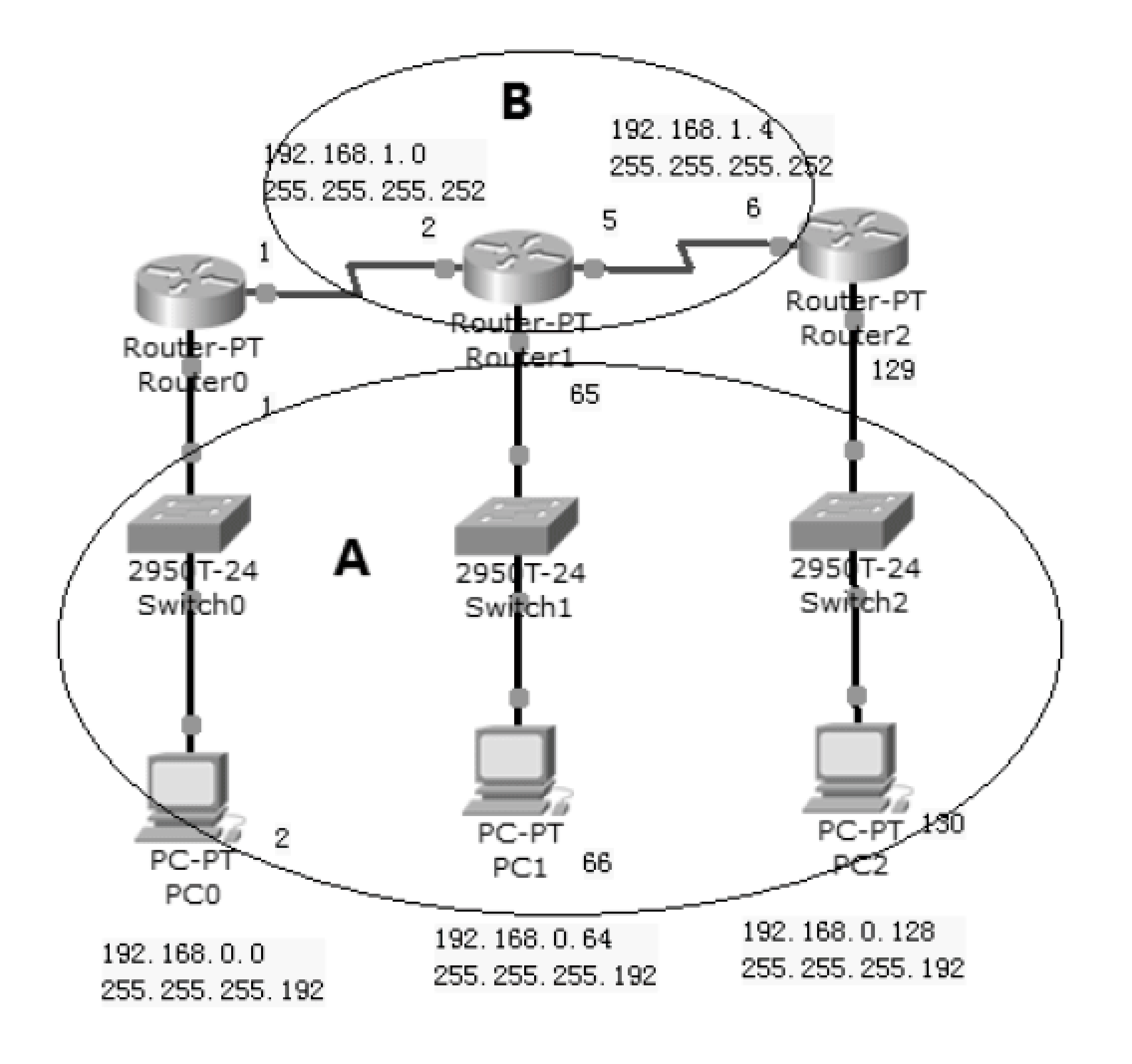
```
Router#show ip route
Gateway of last resort is not set
        192.168.0.0/24 is variably subnetted, 5 subnets, 4 masks
C       192.168.0.0/29 is directly connected, Serial3/0
C       192.168.0.8/29 is directly connected, Serial2/0
R       192.168.0.32/27 [120/1] via 192.168.0.1, 00:00:01, Serial3/0
C       192.168.0.64/26 is directly connected, FastEthernet0/0
R       192.168.0.128/25 [120/1] via 192.168.0.10, 00:00:03, Serial2/0
```

现在学到了网络中的所有网段，你也可以查看 Router0 和 Router2 的路由表。

6.7.2 实验 2：配置 RIPv2 支持不连续子网

打开随书光盘中第 6 章“实验 2 配置 RIPv2 支持不连续子网.pkt”，网络拓扑如图 6-26 所示。A 区域是 192.168.0.0/24 这个 C 类网络划分的子网被 B 区域 192.168.1.0/24 这个 C 类划分的子网络给隔开了，对于 192.168.0.0 这个 C 类网络划分的子网就不连续了。网络中的路由器和计算机已经按照图中所示的 IP 地址进行了设置。

这个实验将会验证关闭 RIPv2 的自动汇总，使之支持不连续子网。



▲图 6-26 不连续子网网络拓扑

操作步骤如下。

（1）在 Router0、Router1 和 Router2 上启用 RIP 协议，更改为 RIPv2，运行以下命令。

```
Router (config) #router rip
Router (config-router) #network 192.168.0.0
Router (config-router) #network 192.168.1.0
Router (config-router) #version 2
```

（2）在 Router1 上，查看路由表。

```
Router#show ip route
Gateway of last resort is not set
        192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
R       192.168.0.0/24 [120/1] via 192.168.1.1, 00:00:11, Serial3/0
                    [120/1] via 192.168.1.6, 00:00:12, Serial2/0
C       192.168.0.64/26 is directly connected, FastEthernet0/0
        192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial3/0
C       192.168.1.4 is directly connected, Serial2/0
```

可以看到到 192.168.0.0/24 网段有两个路径，进行了错误的汇总，得到了错误的路由。

（3）在 Router0、Router1 和 Router2 上关闭 RIPv2 自动汇总，运行以下命令。

```
Router (config) #router rip
Router (config-router) #no auto-summary
```

（4）在 Router1 上再次查看路由表。

```
Router#clear ip route *         --该命令用于清除以前通过 RIP 学到的路由
Router#show ip route
Router#show ip route
        192.168.0.0/24 is variably subnetted, 3 subnets, 2 masks
R       192.168.0.0/26 [120/1] via 192.168.1.1, 00:00:07, Serial3/0
C       192.168.0.64/26 is directly connected, FastEthernet0/0
R       192.168.0.128/26 [120/1] via 192.168.1.6, 00:00:00, Serial2/0
        192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial3/0
C       192.168.1.4 is directly connected, Serial2/0
```

关闭自动汇总后，网络中的所有网段都出现了。

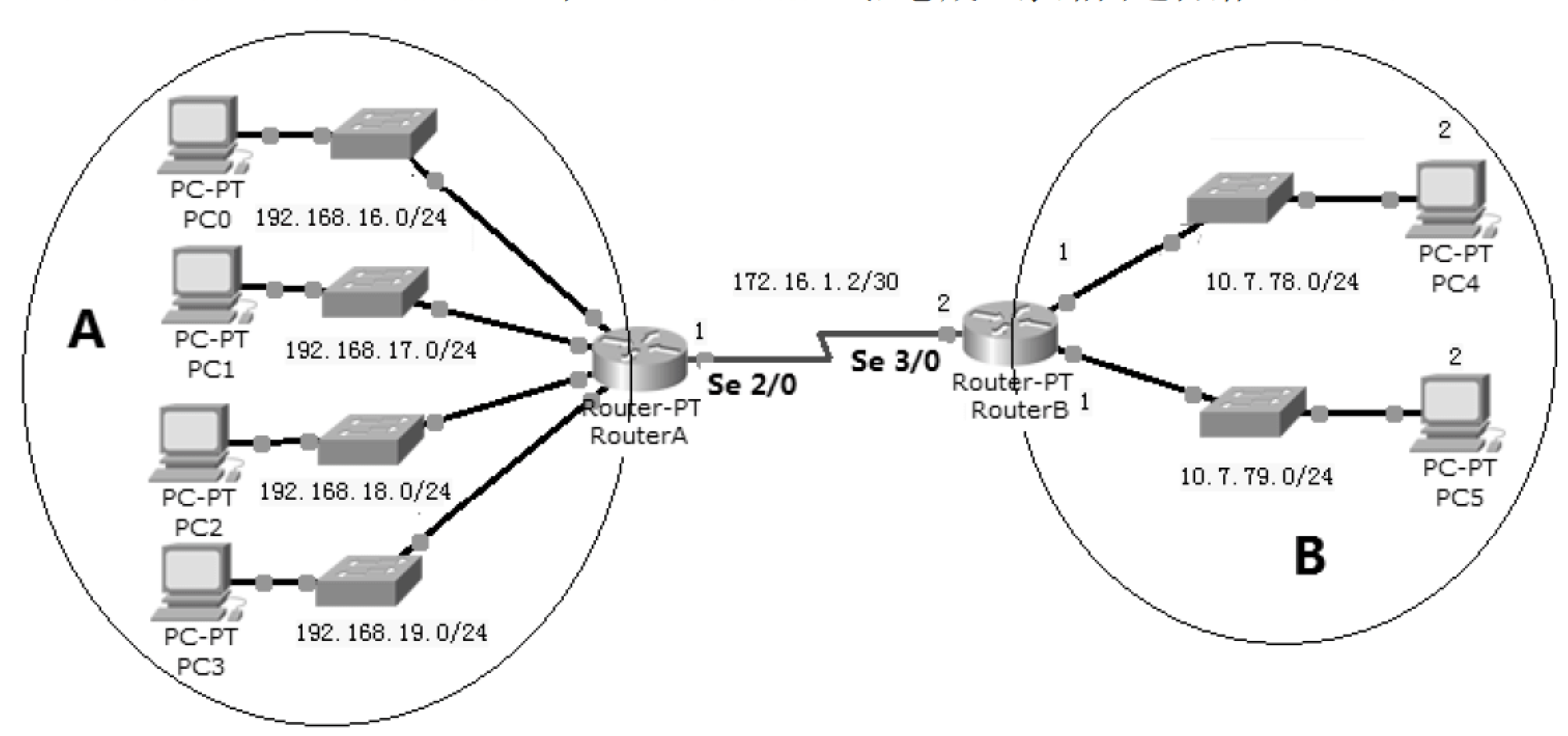
6.7.3 实验 3：配置 EIGRP 手动汇总

EIGRP 会自动在类的边界自动汇总，你可以使用 CIDR 汇总连续的网络。

打开随书光盘中第 6 章“实验 3 配置 EIGRP 手动汇总.pkt”，网络拓扑如图 6-27 所示，网络中的路由器已经配置好了 IP 地址。本实验可以验证 EIGRP 的自动汇总和配置 EIGRP 手动汇总。

可以看到A区域的4个连续的C类网络，可以合并为192.168.16.0/22。B区域是10.0.0.0/8 A类网络划分的两个子网。

你需要在RouterA和RouterB上配置EIGRP。在RouterA上手动将192.168.16.0/24、192.168.17.0/24、192.168.18.0/24和192.168.19.0/24汇总成一条路由通告给RouterB。



▲图 6-27　EIGRP 手动汇总

操作步骤如下。

（1）在RouterA上启用EIGRP。

```
RouterA(config)#router eigrp 10
RouterA(config-router)#network 192.168.16.0
RouterA(config-router)#network 192.168.17.0
RouterA(config-router)#network 192.168.18.0
RouterA(config-router)#network 192.168.19.0
RouterA(config-router)#network 172.16.0.0
```

（2）在RouterB上启用EIGRP。

```
RouterB(config)#router eigrp 10
RouterB(config-router)#network 172.16.0.0
RouterB(config-router)#network 10.0.0.0
```

（3）在RouterB上查看路由表。

```
RouterB#show ip route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D    10.0.0.0/8 is a summary, 00:00:29, Null0
C    10.7.78.0/24 is directly connected, FastEthernet0/0
C    10.7.79.0/24 is directly connected, FastEthernet1/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
```

```
D    172.16.0.0/16 is a summary, 00:00:29, Null0
C    172.16.1.0/30 is directly connected, Serial3/0
D    192.168.16.0/24 [90/20514560] via 172.16.1.1, 00:00:38, Serial3/0
D    192.168.17.0/24 [90/20514560] via 172.16.1.1, 00:00:38, Serial3/0
D    192.168.18.0/24 [90/20514560] via 172.16.1.1, 00:00:38, Serial3/0
D    192.168.19.0/24 [90/20514560] via 172.16.1.1, 00:00:38, Serial3/0
```

学到了 192.168.16.0/24、192.168.17.0/24、192.168.18.0/24 和 192.168.19.0/24 四个网段的路由，需要手动汇总。

（4）在 RouterA 上进行手动汇总。

```
RouterA (config) #interface serial 2/0
RouterA (config-if) #ip summary-address eigrp 10 192.168.16.0 255.255.252.0
```

（5）在 RouterB 上查看路由表。

```
RouterB#show ip route
Gateway of last resort is not set
        10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
D       10.0.0.0/8 is a summary, 00:09:13, Null0
D       10.7.78.0/23 is a summary, 00:00:34, Null0
C       10.7.78.0/24 is directly connected, FastEthernet0/0
C       10.7.79.0/24 is directly connected, FastEthernet1/0
        172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:09:13, Null0
C       172.16.1.0/30 is directly connected, Serial3/0
D       192.168.16.0/22 [90/20514560] via 172.16.1.1, 00:00:34, Serial3/07
                                                        --汇总成一条
```

可以看到到达 A 区域 4 个 C 类网络的路由汇总成一条。

（6）在 RouterA 上查看路由表。

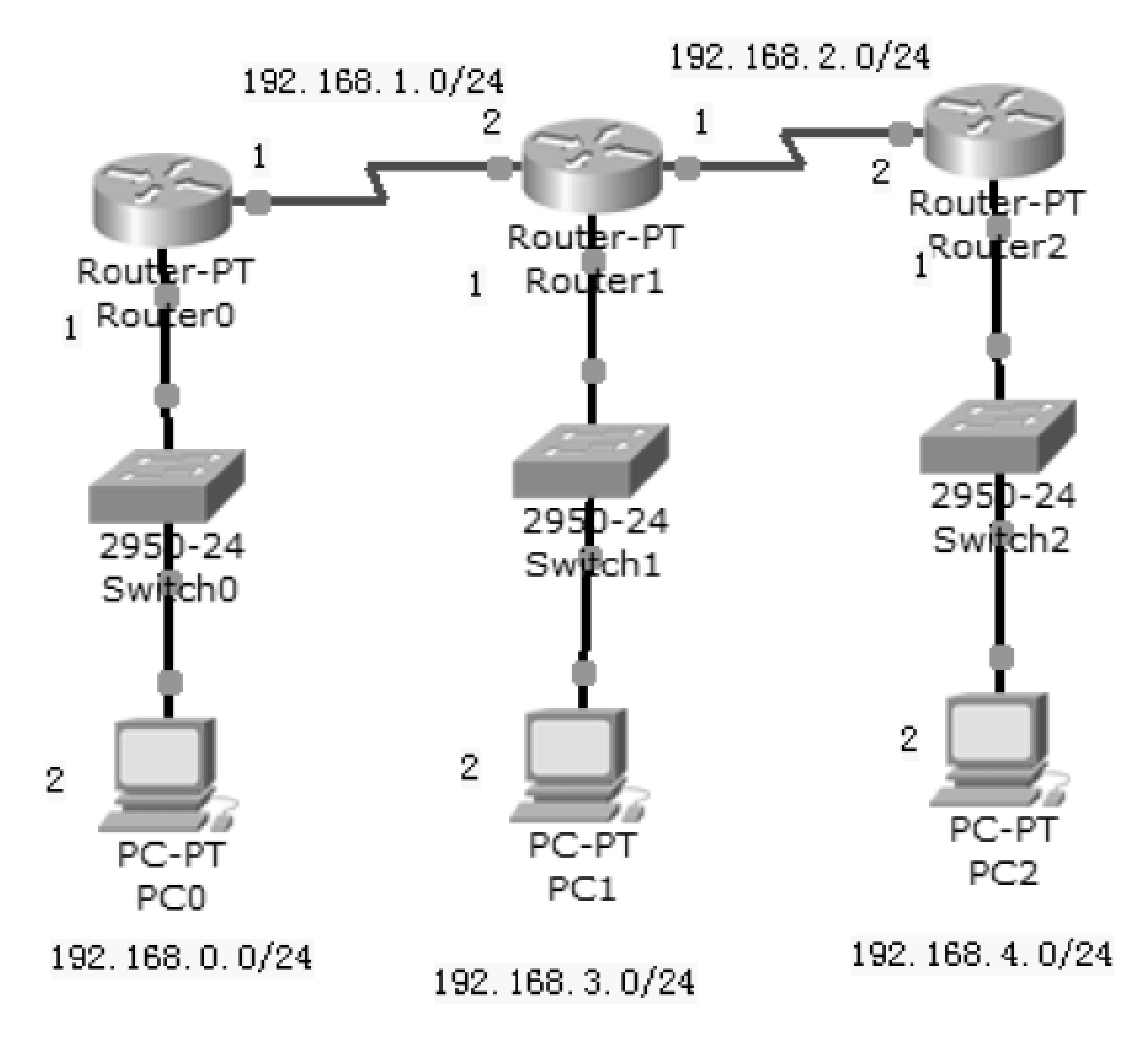
```
RouterA#show ip route
D    10.0.0.0/8 [90/20514560] via 172.16.1.2, 00:14:27, Serial2/0
                                                        --将 B 区域自动汇总
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D    172.16.0.0/16 is a summary, 00:24:16, Null0
C    172.16.1.0/30 is directly connected, Serial2/0
     192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.16.0/22 is a summary, 00:16:44, Null0
C    192.168.16.0/24 is directly connected, FastEthernet0/0
C    192.168.17.0/24 is directly connected, FastEthernet1/0
C    192.168.18.0/24 is directly connected, FastEthernet4/0
```

```
C    192.168.19.0/24 is directly connected, FastEthernet5/0
```

看第一条路由，EIGRP 默认在类的边界自动汇总，将 B 区域的两个子网自动汇总为一条。

6.7.4　实验 4：OSPF 排错

打开随书光盘中第 6 章“实验 4　OSPF 排错.pkt”，网络拓扑如图 6-28 所示，网络中的计算机和路由器已经配置好了 IP 地址，3 个路由器都配置了 OSPF 协议，工作在 area 0。但是 PC0 不能 ping 通 PC2，你需要快速找到 OSPF 配置的错误并改正。



▲图 6-28　网络拓扑

操作步骤如下。

（1）在所有的路由器上运行以下命令，查看 OSPF 的配置。

```
Router#show ip protocols
```

注意观察 network 和 area 的配置是否正确。如果有错误，改正。

（2）改正后在所有的路由器上运行以下命令查看路由表。

```
Router#show ip route
```

6.8　习 题

1. 路由信息协议 RIP 是内部网关协议 IGP 中使用得最广泛的一种基于＿（1）＿的协议，其最大的优点是＿（2）＿。RIP 规定数据每经过一个路由器，跳数增加 1。实际使用中，一个通路上最多可包含的路由器数量是＿（3）＿，更新路由表的原则是：使到各目的网络的＿（4）＿。更新路由表的依据是：若相邻路由器说：“我到目的网络 Y 的距离为 N”，则收到此信息的路由器 K 就知道：“若将下一站路由器

选为 X，则我到网络 Y 的距离为___（5）___”。

（1） A. 链路状态路由算法　　B. 距离矢量路由算法
　　C. 集中式路由算法　　D. 固定路由算法
（2） A. 简单　　B. 可靠性高
　　C. 速度快　　D. 功能强
（3） A. 1 个　　B. 16 个
　　C. 15 个　　D. 无数个
（4） A. 距离最短　　B. 时延最小
　　C. 路由最少　　D. 路径最空闲
（5） A. N　　B. N－1
　　C. 1　　D. N+1

2. 在 RIP 协议中，默认的路由更新周期是______秒。
A. 30　　B. 60　　C. 90　　D. 100

3. 以下协议中支持可变长子网掩码（VLSM）和路由汇聚功能（Route Summarization）的是_____。
A．IGRP　　B．OSPF　　C．VTP　　D．RIPv1

4. 对路由选择协议的一个要求是必须能够快速收敛，所谓“路由收敛”是指_____。
A．路由器能把分组发送到预定的目标
B．路由器处理分组的速度足够快
C．网络设备的路由表与网络拓扑机构保持一致
D．能把多个子网汇聚成一个超网

5. 以下关于 OSPF 协议的描述中，最准确的是_____。
A．OSPF 协议根据链路状态法计算最佳路由
B．OSPF 协议是用于自治系统之间的外部网关协议
C．OSPF 协议不能根据网络通信情况动态地改变路由
D．OSPF 协议只能适用于小型网络

6. RIPv1 与 RIPv2 的区别是____。
A．RIPv1 是距离矢量路由协议，而 RIPv2 是链路状态路由协议
B．RIPv1 不支持可变长子网掩码，而 RIPv2 支持可变长子网掩码
C．RIPv1 每隔 30 秒广播一次路由信息，而 RIPv2 每隔 90 秒广播一次路由信息
D．RIPv1 的最大跳数为 15，而 RIPv2 的最大跳数为 30

7. 关于 OSPF 协议，下面的描述中不正确的是____。
A．OSPF 是一种链路状态协议
B．OSPF 使用链路状态公告（LSA）扩散路由信息
C．OSPF 网络中用区域 1 来表示主干网段
D．OSPF 路由器中可以配置多个路由进程

习题答案

1.（1）B （2）A （3）C （4）C （5）D

2. A

3. B

4. C

5. A

6. B

7. C

第 7 章　交　换

本章介绍交换机、集线器和网桥设备的区别，交换机如何优化网络，设计高可用的交换网络，交换机阻断环路的生成树技术，交换机端口安全。

介绍什么是 VLAN（虚拟局域网），如何创建 VLAN，以及将相应的接口指定到特定的 VLAN，配置干道链路和 VLAN 间路由。使用 VTP（VLAN 间干道协议）协议简化 VLAN 管理。

本章主要内容：

- 使用交换机优化网络
- 设计高可用的交换网络
- 生成树协议
- 配置交换机的端口安全
- 配置监视端口
- 创建和管理 VLAN
- 使用 VTP 协议简化 VLAN 管理
- 设置 VLAN 间路由
- 交换机 etherchannel

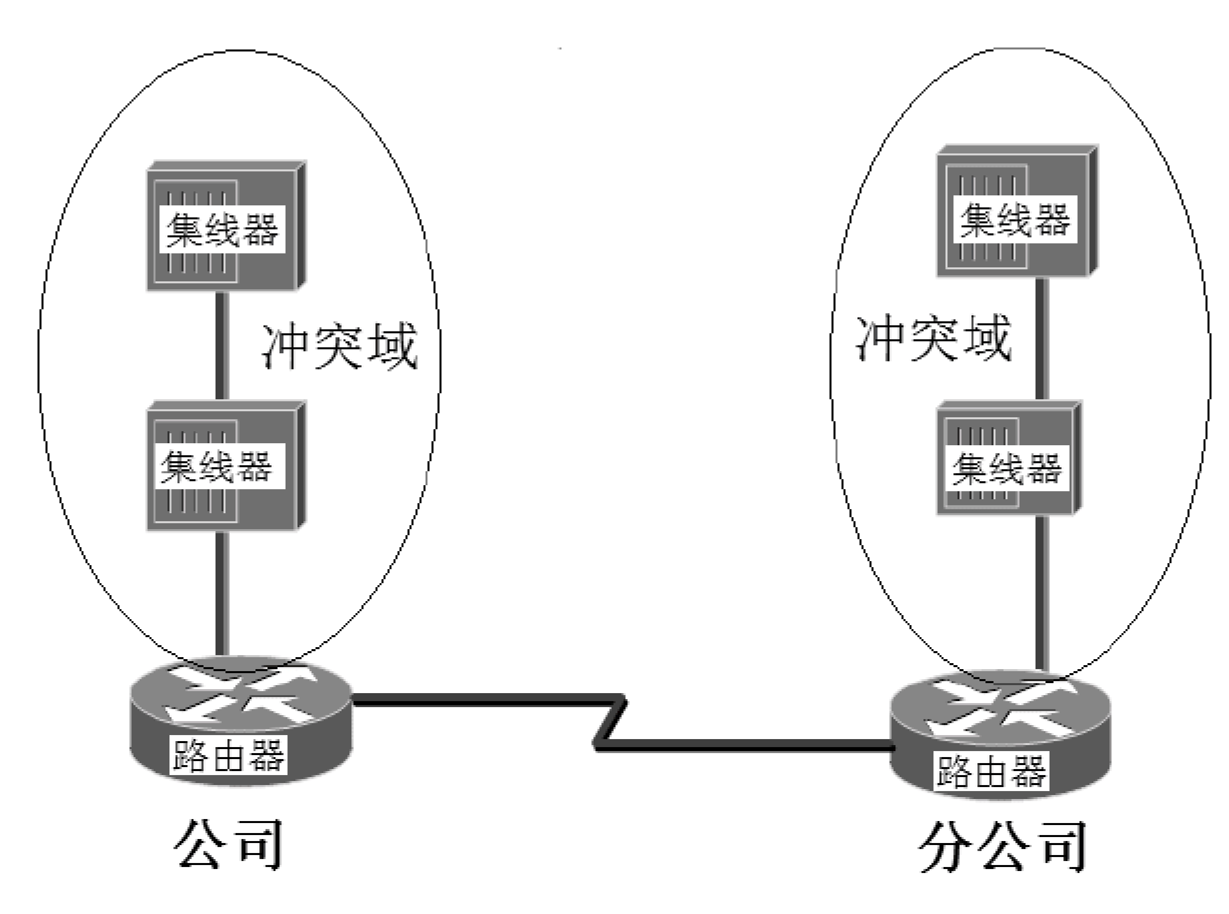
7.1 局域网组网设备

本章提及的交换，都是指的二层交换，除非另有所指。下面讲解局域网组网技术的发展过程，将会为大家介绍集线器、网桥和交换机的特点。

7.1.1 集线器

我们在第 1 章讲过，集线器连接的网络是一个大的冲突域。集线器上的两个结点通信，虽然数据帧目标 MAC 地址和源 MAC 很明确，但是集线器还是将该数据帧扩散到所有的端口，这样就影响了集线器上其他的结点进行数据通信，因此说集线器连接的网络是一个冲突域。

如图 7-1 所示，网段中计算机的数量增多，需要两个集线器连接起来以确保有更多的接口连接计算机，这样使得冲突域增大。集线器连接的网络共享带宽，如果 10M 的以太网连接 10 台计算机，每个计算机平均得到 1M 带宽，但是随着计算机数量、冲突的增加，每个计算机得到的带宽会小于平均带宽。



▲图 7-1　集线器连接的网络

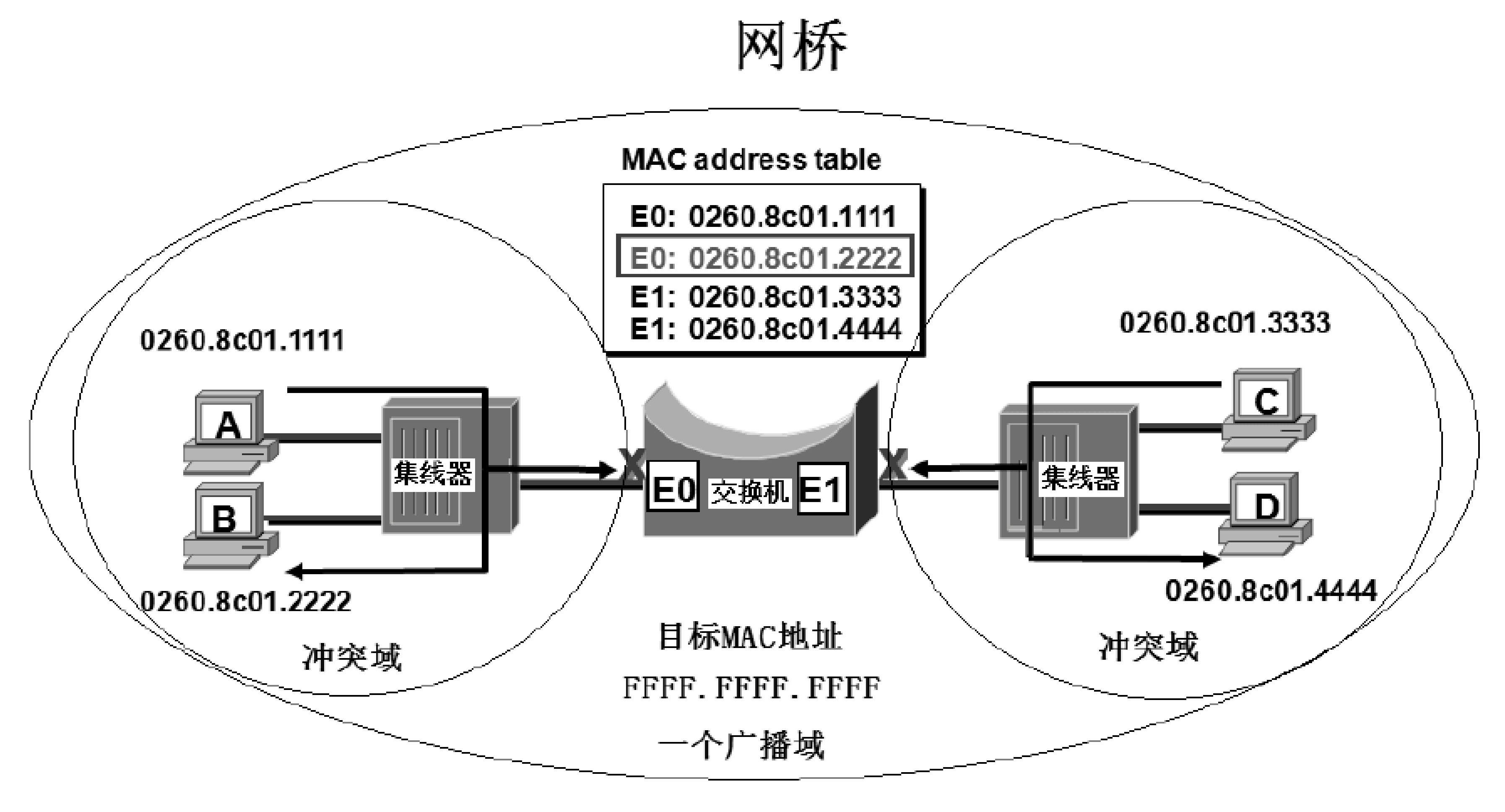
有没有办法将集线器组网产生的大的冲突域减小？有，那就是在网络中使用网桥优化集线器连接的网络。

7.1.2 网桥

在两个集线器之间连接一个网桥，网桥能够基于 MAC 地址表转发数据。如图 7-2 所示，网桥有两个以太网接口 E0 和 E1，并且知道 E0 对应哪些 MAC 地址，E1 对应哪些 MAC 地址。当计算机 A 给计算机 B 发送一个数据帧，集线器将该数据帧扩散到所有的接口，网桥的 E0 接口收到该数据帧，查看目标 MAC 地址 0260.8c01.222，该目标 MAC 对应 E0 接口，于是不转发到 E1 接口，这样就不影响计算机 C 和计算机 D 计算机的通信。

网桥将一个大的冲突域划分成两个冲突域，冲突域的数量增加了，但是冲突域减小了。网桥的一个接口就是一个冲突域。

如果网络中的计算机发送一个目标 MAC 地址为 FFFF.FFFF.FFFF 的数据帧，这样的数据帧称为广播，比如 ARP 协议就是使用广播解析对方 MAC 地址的，网桥会将这样的帧转发到除了发送端口的所有端口。所有的端口在同一个广播域。



▲图 7-2　网桥优化网络

网桥基于数据帧的源地址构建 MAC 地址表。刚接入到网上的网桥 MAC 地址表是空的，这时计算机 A 给计算机 B 发送数据帧，网桥接口 E0 将收到该数据帧，并将该数据帧发送到网桥的所有接口，与此同时，将会在 MAC 地址表中记录 E0:026.8c01.1111。计算机 B 给计算机 A 发送数据帧，网桥不会将该数据帧转发到 E1 端口，因为在 MAC 地址表中已经有关于到计算机 A 的 MAC 地址，同时也会在 MAC 地址表中记录 E0:026.8c01.2222。

7.1.3　交换机

交换机（Switch）是高性能的网桥，交换机可以看做是多端口的网桥。网桥是基于软件，而交换机基于硬件，因为交换机使用 ASIC 芯片来帮助它做出数据帧转发的决定。构建 MAC 地址的过程和网桥一样，交换机可以“学习”MAC 地址，并将其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

如图 7-3 所示，交换机和集线器相比有以下优点。

- 交换机的每一个端口是一个冲突域。
- 交换机的端口独享带宽。
- 交换机比集线器安全。

交换机
1 2 3 4
- 交换机的每一个端口是一个冲突域
- 基于数据帧的MAC地址转发数据
- 所有的端口在同一个广播域

▲图 7-3　交换机的作用

将目标 MAC 地址为 FF-FF-FF-FF-FF-FF 的数据帧发送到所有交换机的端口（除了发送端口外），因此交换机连接的网络是一个广播域。

交换机有以下功能。

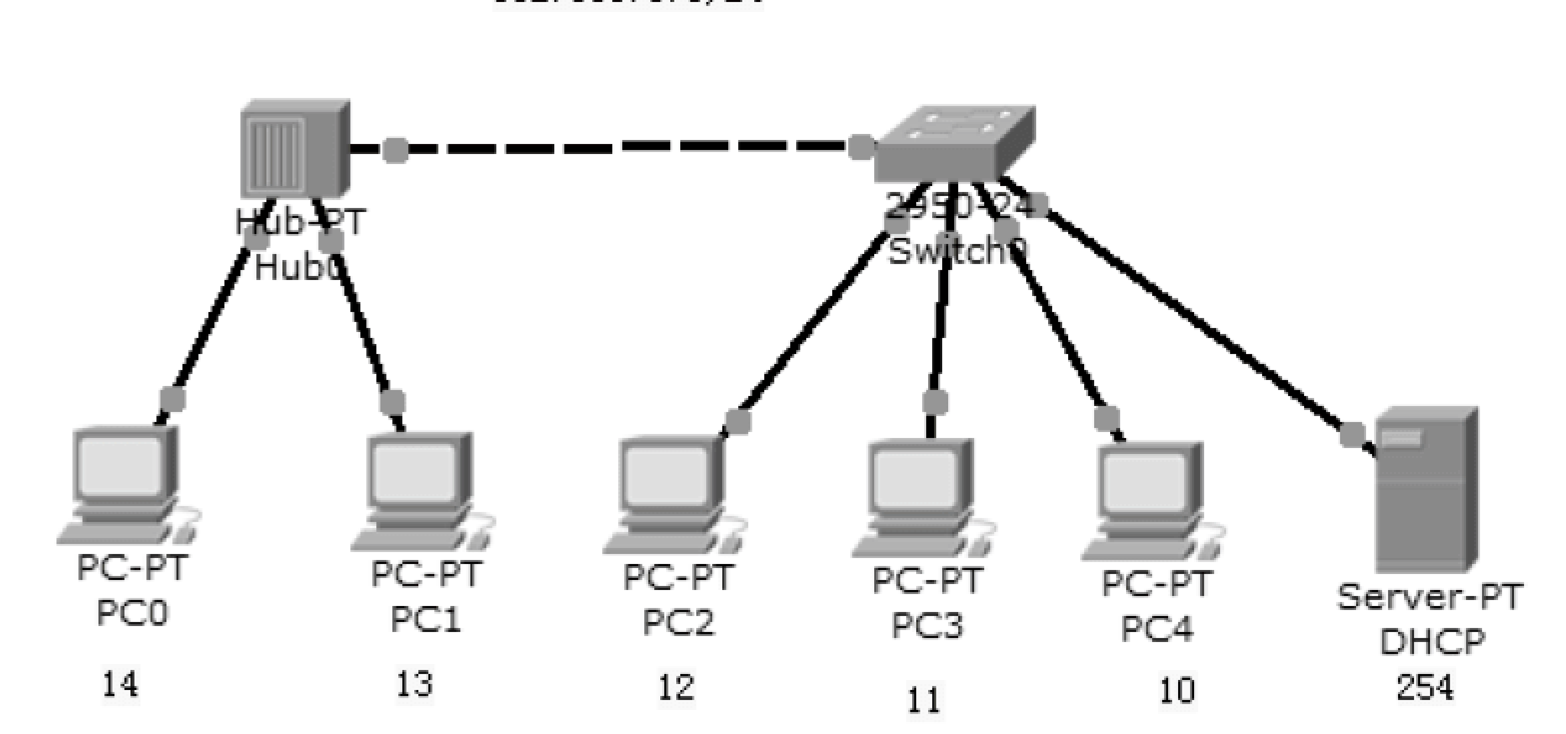
- 构建 MAC 地址表，即地址学习。
- 转发/过滤功能。

如果为了提供冗余而在交换机之间创建了多个连接，网络中可能出现环路。通过使用生成树协议（Spanning Tree Protocol，STP）可以防止产生网络环路，避免广播风暴。

7.1.4 查看交换机的 MAC 地址表

打开随书光盘中第 7 章练习“01 查看交换机的 MAC 地址表.pkt”，网络拓扑如图 7-4 所示，网络中的交换机直连着 3 个计算机、1 个 DHCP 服务器和一个集线器，集线器又连接着两台计算机。网络中的计算机已经按照图示的地址配置完成。

你需要在 PC4 上 ping PC1、 PC2、 PC3、 PC0 和 DHCP，然后查看交换机上的 MAC 地址表，通过查看 MAC 地址表确认交换机的哪个接口连接集线器。



▲图 7-4 查看交换机的 MAC 地址表

操作步骤如下。

（1）在 PC4 上 ping PC1、PC2、PC3、PC0 和 DHCP 的 IP 地址。

（2）在交换机上查看 MAC 地址表。

```
Switch>en      --交换机的配置命令和路由器类似，输入 enable 进入特权模式
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0000.0c7c.7e49    DYNAMIC     Fa0/1
   1    0001.63c6.e338    DYNAMIC     Fa0/5
   1    0030.a336.362b    DYNAMIC     Fa0/4
   1    0030.a3e4.e4c6    DYNAMIC     Fa0/4
```

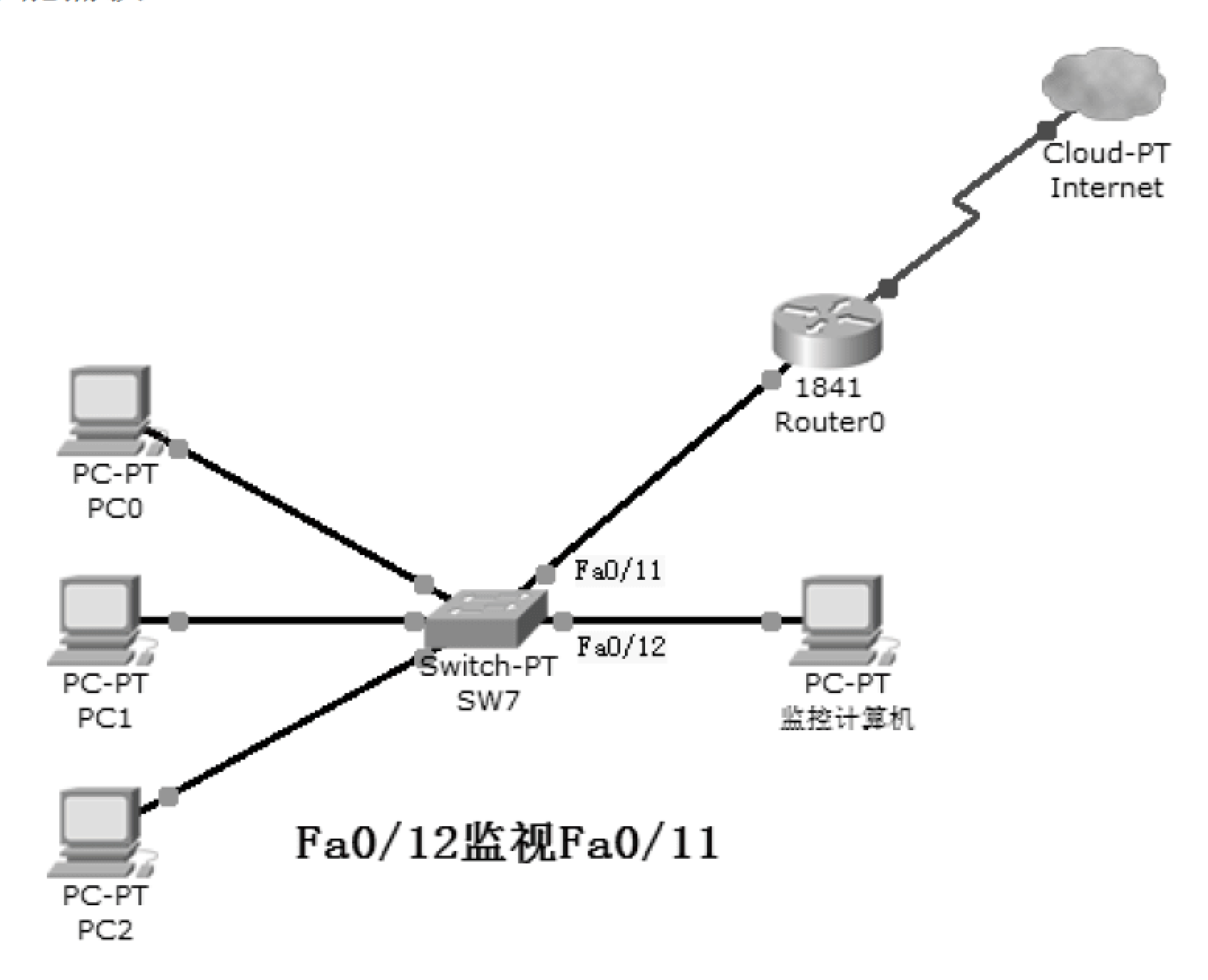
```
    1     0090.0cd7.65c8     DYNAMIC      Fa0/2
    1     00d0.ffce.0eb4      DYNAMIC     Fa0/3
```

通过以上 MAC 地址表可以看到，Fa0/4 接口对应着两个 MAC 地址，可以断定该接口连接集线器。

7.1.5 交换机上配置监控端口

交换机是基于 MAC 地址转发数据包的，比起集线器来说更安全。如图 7-5 所示，在交换机组建的网络中的监控计算机上安装数据包捕获软件，用以监控和分析网络中的流量。监控计算机只能监控自己发出的数据帧、发给自己的数据帧，以及广播和多播数据帧，但是 PC0、PC1 和 PC2 访问 Internet 的流量，监控计算机则不能捕获，因为交换机不向连接监控计算机的端口 Fa0/12 转发数据帧。

如果你想监控 PC0、PC1 和 PC2 访问 Internet 的流量，这些流量都由交换机的 Fa0/11 转发到路由器，如果想让监控计算机捕获到这些流量，你需要配置 Fa0/12 监控 Fa0/11。这样，发送给 Fa0/11 端口的数据帧和来自 Fa0/11 端口的数据，交换机也会发送给 Fa/12 端口，如此捕包软件才能捕获。



▲图 7-5　配置交换机监控端口

1．实验环境

packet Tracer 不支持该实验，因此你只能在物理设备上进行配置和测试。

2．实验目标

配置端口 FastEthernet 12 监视 FastEthernet 11。

3．操作步骤

（1）指定监控端口。监控端口和被监控端口必须属于同一个 session 编号。

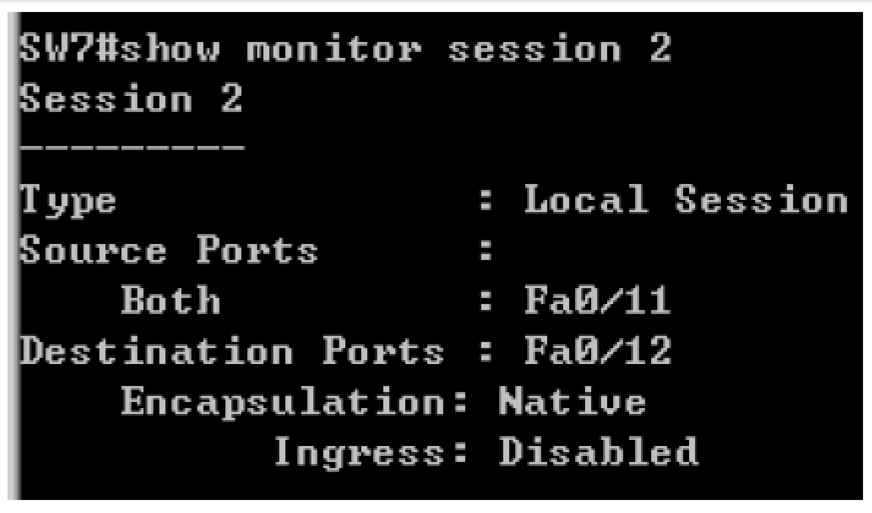
```
SW7（config）#monitor session 2 destination interface FastEthernet 0/12
```

（2）指定被监控端口。

```
SW7（config）#monitor session 2 source interface FastEthernet 0/11
```

（3）查看监控和被监控端口，如图 7-6 所示。

```
SW7#show monitor session 2
```



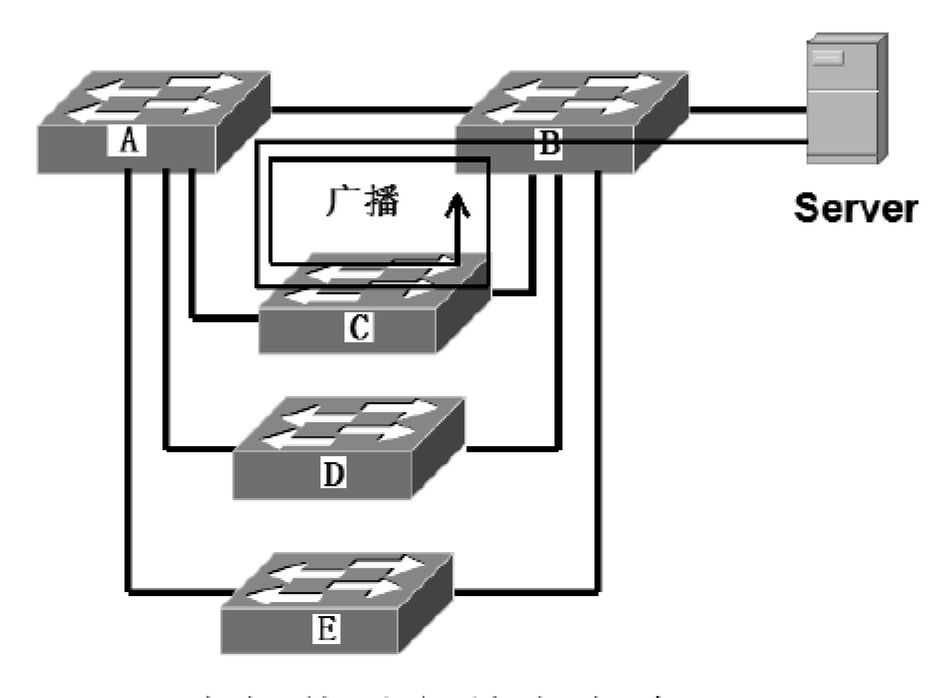
```
SW7#show monitor session 2
Session 2
---------
Type                : Local Session
Source Ports        :
    Both            : Fa0/11
Destination Ports   : Fa0/12
    Encapsulation: Native
          Ingress: Disabled
```

▲图 7-6　查看监控和被监控端口

7.2 生成树协议

如果企业的网络非常重要（比如医院的网络）。为了避免汇聚层和核心层设备故障造成网络故障，可以设计成双核心层和双汇聚层。

如图 7-7 所示，网络交换机 C、D 和 E 是接入层交换机，交换机 A、B 是汇聚层交换机，很显然是双汇聚层。



- 冗余拓扑避免单点失败
- 冗余拓扑产生广播风暴
- 冗余拓扑产生MAC地址表混乱

▲图 7-7　冗余拓扑

这样网络中就有很多环路，如果 Server 发送一个广播数据帧，该数据帧将会在任意一个环路中无休止地转发，造成广播风暴，网络堵塞。

如何既能实现网络有冗余拓扑，又能避免环路。这就需要讲到交换机的一个重要的功能，也即下面要介绍的交换机生成树协议。

7.2.1 生成树协议

生成树协议（STP）最早是由数字设备公司（Dig ital Equipment Corporation，DEC）开发的，这个公司后来被收购并改名为 Compaq 公司。IEEE 后来开发了它自己的 STP 版本，称为 802.1D。Cisco 交换机默认运行 STP 的 IEEE 802.1D 版本，它与 DEC 版本不兼容。Cisco 在其新出品的交换机上使用了另一个工业标准，称为 802.1w，这一节介绍 STP，但先要定义一些有关 STP 的重要而基本的概念。

STP 的主要任务是阻止在第 2 层网络（网桥或交换机）上产生网络环路。它警惕地监控着网络中的所有链路，通过关闭任何冗余的接口来确保在网络中不会产生环路。STP 采用生成树算法 STA（Spanning Tree Algorithm），它首先创建一个拓扑数据库，然后搜索并破坏掉冗余的链路。运行了 STA 算法之后，帧就只能被转发到保险的、由 STP 挑选出来的链路上。

7.2.2 生成树术语

在详细讨论 STP 怎样在网络中起作用之前，需要理解一些基本的概念和术语，以及它们是怎样与第 2 层交换式网络联系在一起的（下面提到的桥就理解为交换机）。

- 根桥（Rootbridge）：是桥 ID 最低的网桥，也就是根交换机。对于 STP 来说，关键的问题是为网络中所有的交换机推选一个根桥，并让根桥成为网络中的焦点。在网络中，所有其他的决定（比如哪一个端口要被阻塞，哪一个端口要被置为转发模式）都是根据根桥的判断来做出选择的。
- 桥协议数据单元（Bridge Protocol Data Unit，BPDU）：所有的交换机相互之间都交换信息，并利用这些信息来选出根交换机或进行网络的后续配置。每台交换机都对 BPDU 中的参数进行比较，它们将 BPDU 传送给某个邻居，并在其中放入它们从其他邻居那里收到的 BPDU。
- 桥 ID（BridgeID）：STP 利用桥 ID 来跟踪网络中的所有交换机。桥 ID 是由桥优先级（在所有的 Cisco 交换机上，默认的优先级为 32768）和 MAC 地址的组合来决定的。在网络中，桥 ID 最小的网桥就称为根桥。
- 非根桥（Nonrootbridge）：除了根桥外，其他所有的网桥都是非根桥。它们相互之间都交换 BPDU，并在所有交换机上更新 STP 拓扑数据库，以防止环路，并对链路失效采取补救措施。
- 端口开销（Portcost）：当两台交换机之间有多条链路且都不是根端口时，就根据端口开销来决定最佳路径。链路的开销取决于链路的带宽。
- 根端口（Rootport）：是指直接连到根桥的链路所在的端口，或者到根桥的路径最短的端口。如果有多条链路连接到根桥，就通过检查每条链路的带宽来决定端口的开销，开销最低的端口就成为根端口。如果多条链路的开销相同，就使用桥 ID 小一些的那个桥。如果多条链路来自同一台设备，就使用端口号最低的那条链路。
- 指定端口（Designated Port）：有最低开销的端口就是指定端口，指定端口被标记为转发端口。

- 非指定端口（Nondesignated Port）：是指开销比指定端口高的端口，非指定端口将被置为阻塞状态，它不是转发端口。
- 转发端口（Forwarding Port）：是指能够转发帧的端口。
- 阻塞端口（Blocked Port）：是指不能转发帧的端口，这样做是为了防止产生环路。然而，被阻塞的端口将始终监听帧。

7.2.3 生成树的操作

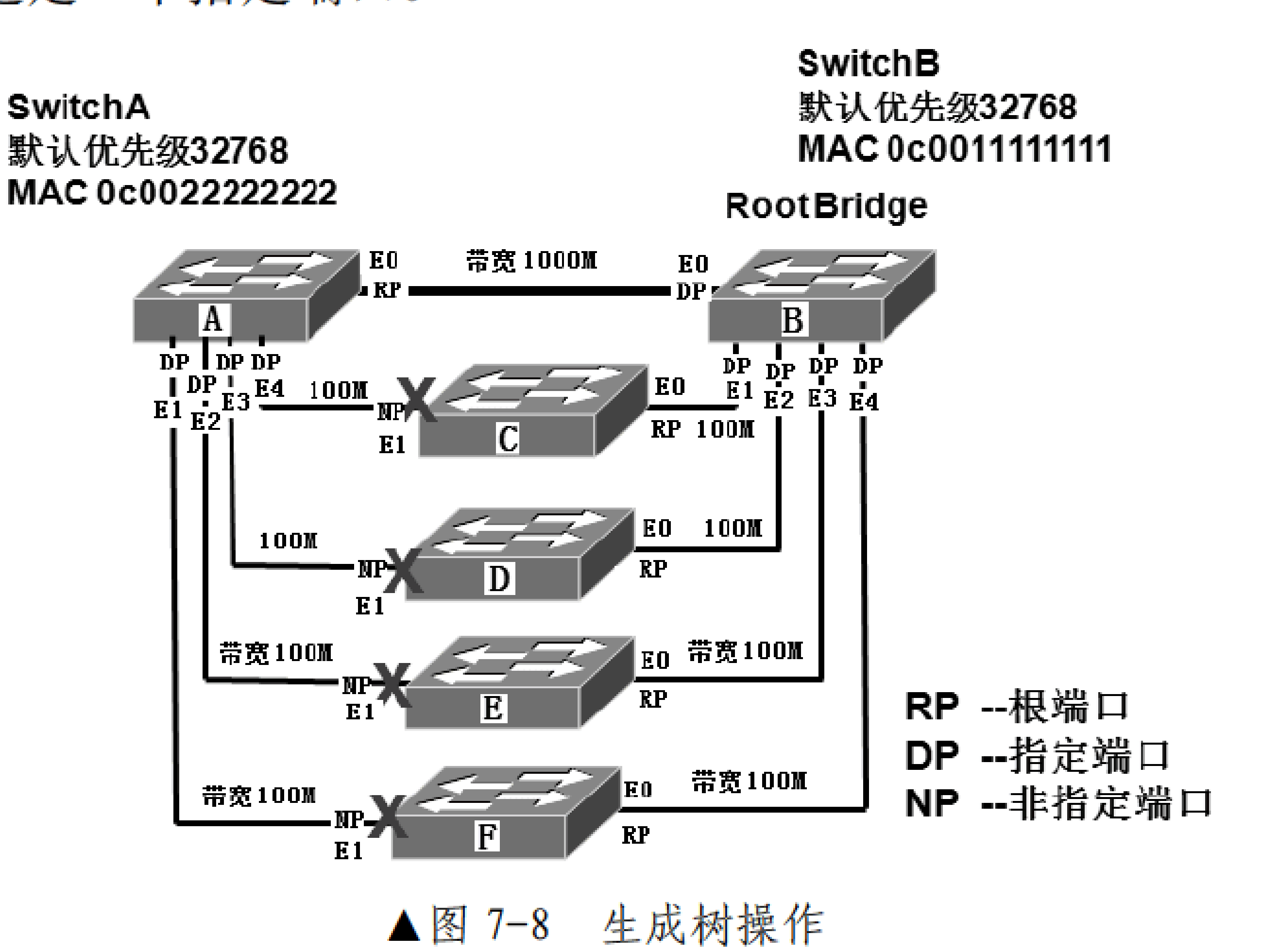
正如前面提到的，STP 的任务是找到网络中的所有链路，并关闭任何冗余的链路，这样就可以防止网络环路的产生。为了达到这个目的，STP 首先需要选举一个根桥，由根桥来负责决定网络拓扑。一旦所有的交换机都同意将某台交换机选举为根桥，其余的交换机就必须找到其唯一的根端口。在两台交换机之间的每一条链路必须有唯一的指定端口，在那条链路上的端口提供到根桥最大的带宽。

下面将以如图 7-8 所示的网络设备讲解生成树的过程。生成树的操作分为以下三步。

（1）选举根桥。

（2）非根桥交换机确定根端口。

（3）每个链路选定一个指定端口。



▲图 7-8　生成树操作

1. 选举根桥

在以上网络中有 A、B、C、D、E 和 F 六个路由器，网桥 ID 最小的将被选举为根桥。网桥 ID 为 8 个字节长，其中包括设备的优先级和 MAC 地址，在运行 IEEE STP 版本的所有设备上，默认优先级都为 32768。优先级相同，MAC 地址最小的将被选举为根桥。

默认每隔 2 秒钟发送一次 BPDU，它被发送到网桥/交换机的所有活动端口上，通过 BPDU 选举根桥。在本例中，交换机 A 和交换机 B 优先级相同，交换机 B 的 MAC 地址为 0c0011111111，比交换机 A 的 MAC 地址 0c0022222222 小，交换机 B 就更加有可能成为根桥。你可以更改交换机的优先级，来指定成为根桥的首选和备用交换机。在本示例中很显然让交换机 A 和交换机 B 成为首选和备用根交换机最好，因为这两个交换机为汇聚层交换机。

本示例假设交换机 B 是所有交换机中 MAC 地址最小的，选举为根网桥。

2．选举根端口

确定了根网桥后，交换机 A、C、D、E 和 F 为非根桥，这些交换机需要查看哪些端口到根交换机距离近，带宽越高距离就越近。对于 C 交换机来说到达根网桥最近的端口是 E0。因此 E0 接口就被选举为根端口。根端口转发数据帧。

3．选举指定端口

直白一点来说，就是每根网线，都要比较看哪一端距离根桥近。距离根桥近的那一端连接的端口为指定端口。由于 A 和 B 交换机之间的连接带宽为 1000M，因此 A 交换机的 E1、E2、E3 和 E4 端口比交换机 C、D、E 和 F 的 E1 端口距离根桥近，因此 A 交换机的 E1、E2、E3 和 E4 端口成为指定端口。根桥的所有端口都是指定端口。指定端口转发数据帧。

4．非指定端口

确定了根端口和指定端口，剩下的端口就是非指定端口，非指定端口将被置为阻塞状态，不是转发端口。本示例交换机 C、D、E 和 F 的 E1 接口就是非指定端口。虽然不能转发帧，但仍然可以接收帧，包括 BPDU。

提示	网络中如果有集线器设备，则集线器设备不参与生成树。

7.2.4 生成树的端口状态

对于运行 STP 的网桥或交换机来说，其端口状态会在下列 5 种状态之间转变。

- 阻塞（Blocking）：被阻塞的端口将不能转发帧，它只监听 BPDU。设置阻塞状态的意图是防止使用有环路的路径。当交换机加电时，默认情况下所有的端口都处于阻塞状态。
- 侦听（Listening）：端口都侦听 BPDU，以确信在传送数据帧之前，在网络上没有环路产生。侦听状态的端口，在没有形成 MAC 地址表时，就准备转发数据帧。
- 学习（Learning）：交换机端口侦听 BPDU，并学习交换式网络中的所有路径。处在学习状态的端口形成 MAC 地址表，但不能转发数据帧。转发延迟意味着将端口从侦听状态转换到学习状态所花费的时间，默认设置为 15 秒，可以用命令 showspanning-tree 显示出来。
- 转发（Forwarding）：在桥接的端口上，处在转发状态的端口发送并接收所有的数据帧。 如果在学习状态结束时，端口仍然是指定端口或根端口，它就进入转发状态。
- 禁用（Disabied：从管理上讲，处于禁用状态的端口不能参与帧的转发或形成 STP。处于禁用状态下，端口实质上是不工作的。

说明	只有在学习状态或转发状态下，交换机才能填写 MAC 地址表。

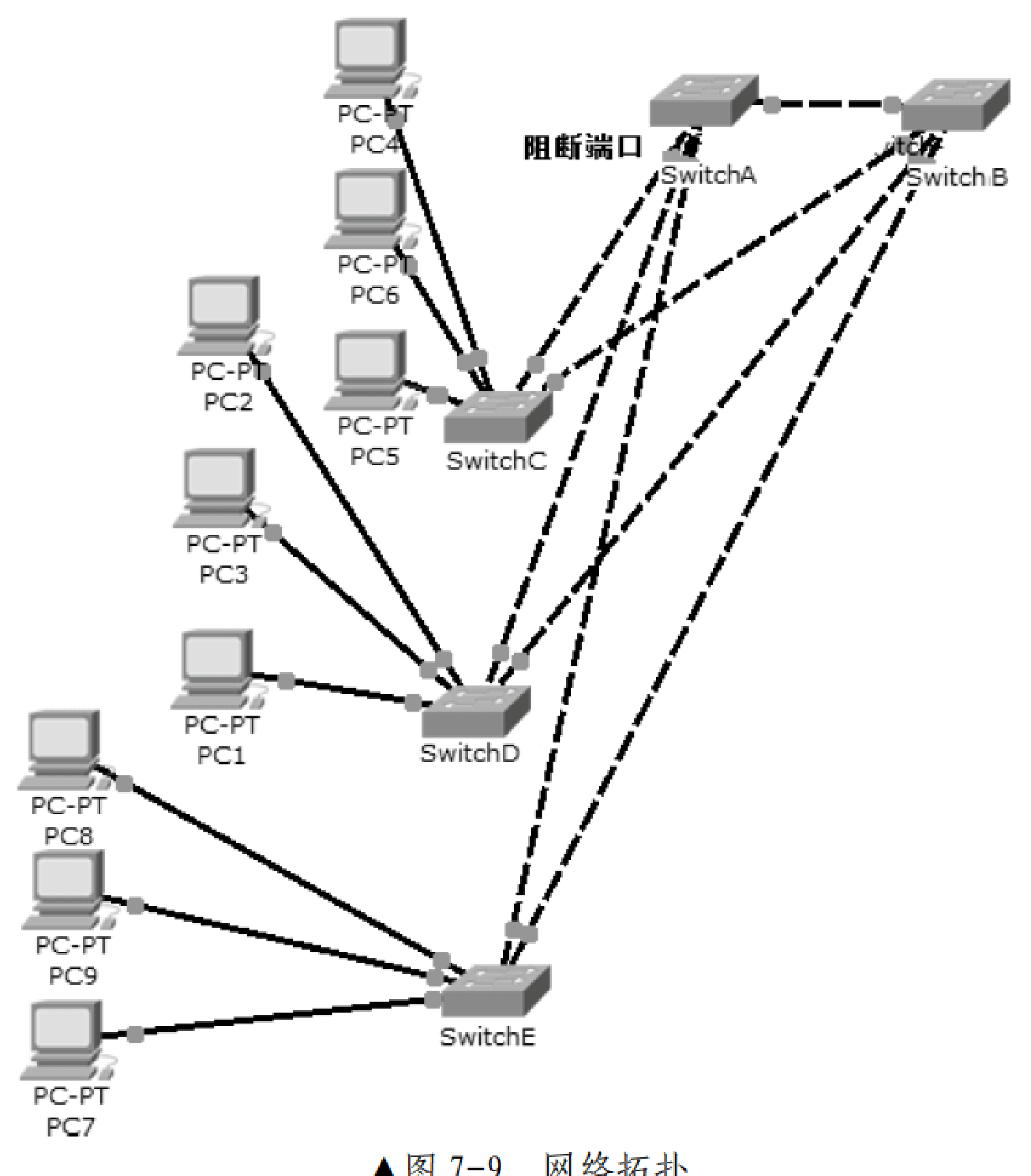
大多数情况下，交换机端口都处在阻塞或转发状态。转发端口是指到根桥的开销最低的端口，但如果网络的拓扑改变（可能是链路失效了，或者有人添加了一台新的交换机），交换机上的端口就会处于侦听或学习状态。

正如前面提到的，阻塞端口是一种防止网络环路的策略。一旦交换机决定了到根桥的最佳路径，那么所有其他的端口将处于阻塞状态。被阻塞的端口仍然能接收 BPDU，它们只是不能发送任何帧。

7.2.5 确认和更改根桥

打开随书光盘中第 7 章练习“02 确认和更改根网桥.pkt”，可以看到网络拓扑如图 7-9 所示，双汇聚层设计，SwitchA 连接 SwitchC、SwitchD 和 SwitchE 的端口，处于阻断状态，可以断定 SwitchA 不是根交换机，因为根交换机的所有端口肯定是转发状态。

你需要确认网络中的根桥。需要指定 SwitchA 作为首选根网桥，SwitchB 作为备用根桥。这就需要更改网桥优先级。



▲图 7-9　网络拓扑

操作步骤如下。

（1）在 SwitchA 上，查看 VLAN 1 的生成树，查看根网桥。

```
Switch>en            --进入特权模式
Switch#show spanning-tree vlan 1 --查看 VLAN 1 的生成树，默认所有接口都在 VLAN1
VLAN0001
  Spanning tree enabled protocol ieee
```

```
  Root ID   Priority   32769          --这是根桥的优先级
            Address    0002.4A63.C9B6   --这是根桥的 MAC 地址
            Cost       4
            Port       6（GigabitEthernet5/1）  --使用 G5/1 这个接口和根桥连接
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority  32769 （priority 32768 sys-id-ext 1）
                                              --这是 SwitchA 的优先级
            Address    00E0.F780.208C               --这是 SwitchA 的 MAC 地址
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
----------- ---------------  --------- -----  ---------------------
Gi5/1           Root FWD 4        128.6    P2P        --FWD 代表转发状态
Gi6/1           Altn BLK 4        128.7    P2P        --BLK 代表阻断状态
Gi7/1           Altn BLK 4        128.8    P2P
Gi8/1           Altn BLK 4        128.9    P2P
```

可以断定 SwitchA 不是根桥，因为 Root ID 和 Bridge ID 不同，网桥 ID 是由优先级和 MAC 地址构成的。

（2）更改 SwitchA 的生成树优先级，使其成为首选根桥。

```
Switch#config t  --进入全局配置模式
Switch（config）#spanning-tree vlan 1 priority ?  --更改 VLAN1 的生成树优先级
  <0-61440>  bridge priority in increments of 4096
                                              --可以看到优先级值的范围
Switch（config）#spanning-tree vlan 1 priority 23   --随便输入一个值
% Bridge Priority must be in increments of 4096.
                                          --提示网桥优先级值增量为 4096
% Allowed values are:                     --显示所有可用的网桥优先级值
  0    4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
Switch（config）#spanning-tree vlan 1 priority 4096
                                          --将网桥优先级的值更改为 4096
```

（3）注意观察网络中的阻断端口发生变化。

（4）在 SwitchA 上运行以下命令，查看新选举的根网桥。

```
Switch#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID   Priority   4097                    --根网桥优先级
```

```
            Address     00E0.F780.208C                 --根网桥 MAC 地址
            This bridge is the root
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority   4097  (priority 4096 sys-id-ext 1)  --网桥优先级
            Address     00E0.F780.208C                     --网桥 MAC 地址
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------- ----------------  --------- -------- ---------------------
Gi5/1           Desg FWD 4        128.6    P2P         --转发状态
Gi6/1           Desg FWD 4        128.7    P2P         --转发状态
Gi7/1           Desg FWD 4        128.8    P2P         --转发状态
Gi8/1           Desg FWD 4        128.9    P2P         --转发状态
```

可以看到更改网桥的优先级后，Root ID 和 Bridge ID 都是 SwitchA 了，这说明 SwitchA 是根桥，并且所有的端口都处于转发状态。

（5）在 SwitchB 上运行以下命令，更改其网桥优先级，将其设置为备用根网桥。

```
Switch (config) #spanning-tree vlan 1 priority 12288
```

7.2.6 关闭 VLAN 1 的生成树

如果你确信网络中的交换机没有环路，并且将来也不会产生环路，可以使用以下命令将 VLAN 1 的生成树关闭。

```
Switch (config) #no spanning-tree vlan 1
```

7.3 优化生成树

当网络中的交换机数量增加或链路有变化时，所有交换机会重新进行生成树操作来确定阻断端口和转发端口。在完成重新计算之前，交换机不能转发任何数据。完成计算之后，才能转发数据，这个过程需要的时间就是生成树的收敛时间。在交换机端口上，生成树拓扑从阻塞到转发的典型收敛时间为 50 秒。也就是说网络拓扑有变化，网络会中断 50 秒。通过将汇聚层或核心层交换机设置为根桥，可以使生成树收敛得又快又好。

7.3.1 生成树快速端口

如果交换机接口连接的是计算机，可以将这些端口设置为快速端口（PortFast），这就意味着，当 STP 正在收敛时，端口不会花费通常的 50 秒才进入转发状态。

打开随书光盘中第 7 章练习“02 确认和更改根网桥.pkt”，在 SwitchC 上，运行以下命令，将连接计算机的接口 FastEthernet 0/1 – FastEthernet 2/1 配置成快速端口。

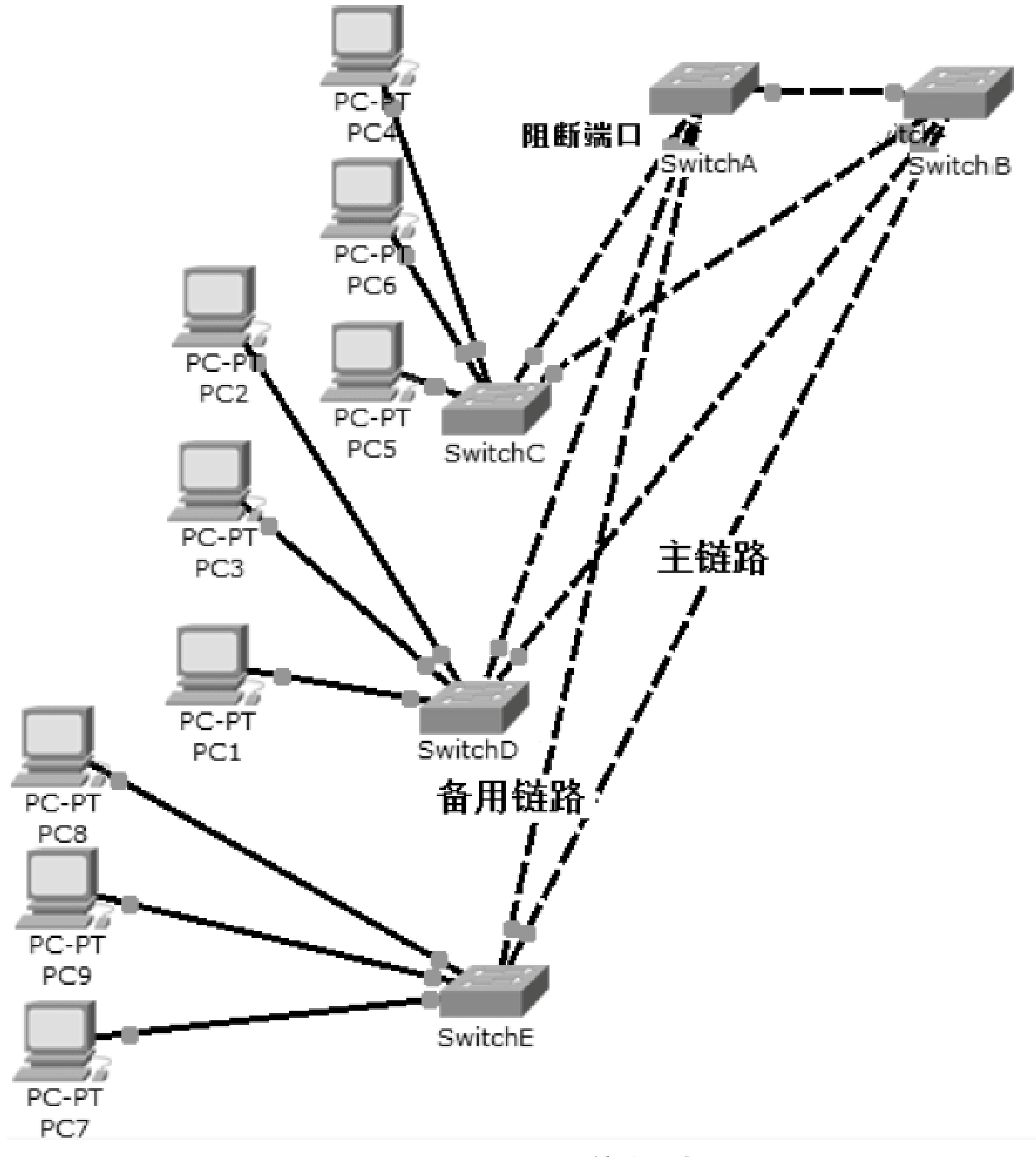
```
Switch（config）#interface range FastEthernet 0/1 - FastEthernet 2/1
Switch（config-if-range）#spanning-tree Portfast
```

如果将一个接口配置快速端口，运行以下命令。

```
Switch（config）#interface range FastEthernet 0/1
Switch（config-if）#spanning-tree Portfast
```

7.3.2 生成树上行链路快速

上行链路快速（UplinkFast）是 Cisco 产品的特性，当链路失效时，它可用来改进 STP 的收敛时间。当交换机至少有一个可选/备份的根端口（处于阻断状态的端口）时，UplinkFast 允许在主链路失效前，找到根的可选路径。这就意味着如果主链路失效，备份链路将被更快启用。如图 7-10 所示，在接入层交换机启用 UplinkFast。如果在 SwitchE 上启用了 UplinkFast，当主链路正常连接时，就已经选好了备用链路，当主链路失效后，备用链路将更快地启用。



▲图 7-10　网络拓扑

在 SwitchE 上启用 UplinkFast：

```
Switch（config）#spanning-tree uplinkfast
```

这是一个全局配置命令，Packet Tracer 软件模拟的交换机则不支持。

7.3.3 启用快速生成树协议（RSTP）802.1w

你可以更改生成树协议的模式将其设置成快速生成树协议（Rapid Spanning Tree Protocol，RSTP），这样上面讨论的 PortFast 和 UplinkFast 的功能都内置了。

Cisco 创建了 PortFast、UplinkFast 来“修补”IEEE 802.1d 标准中的漏洞和缺陷。这些改进特性的不足之处仅在于，它们是 Cisco 专用的且需要进行额外的配置。但新的 802.1w 标准（RSTP）将所有这些“问题”都解决了——只需要打开 RSTP 就可以了。重要的是，必须确信网络中所有的交换机都在正确地运行 802.1w 协议。

```
Switch (config) #spanning-tree mode rapid-pvst
```

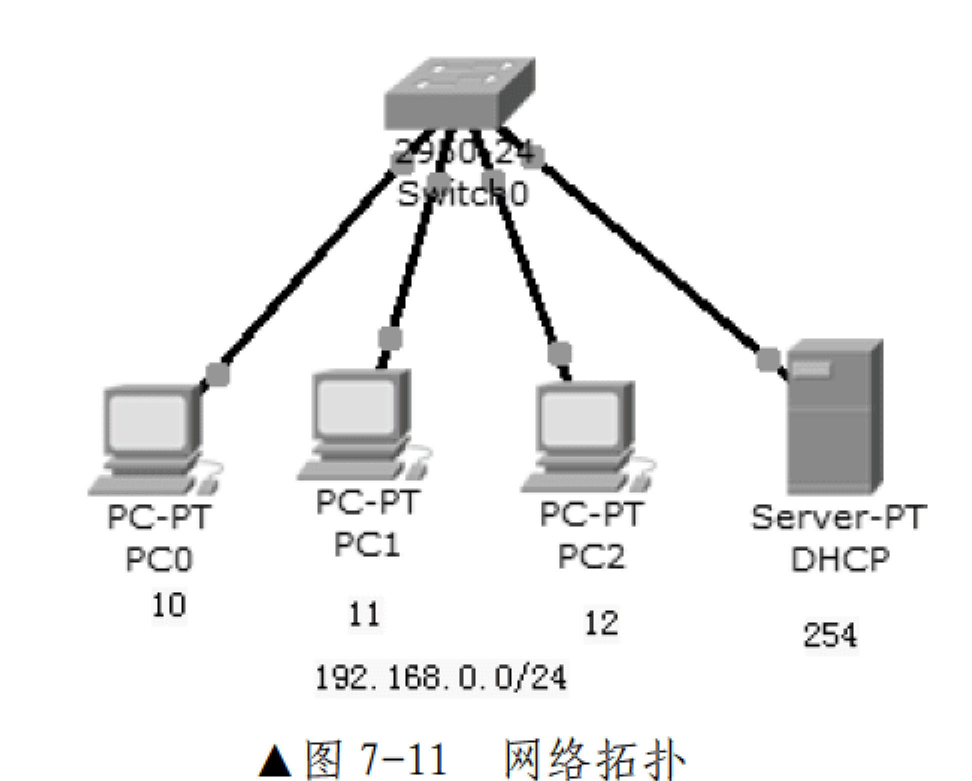
7.4 交换机端口安全

网络对安全要求高的不愿意外单位的人随便将自己的笔记本电脑接入公司的网络。比如河北师大软件学院的教室为本学院学生提供了免费网络接入以便学生能随时访问 Internet 查询资料和学院内网提交作业。突然有一天，发现自习时间，教室里有其他学院的学生接入笔记本电脑上网聊天、玩游戏。如何避免其他学院的学生使用软件学院的网络？这就需要设置交换机的端口和计算机进行绑定，实现交换机端口的安全。

7.4.1 端口和 MAC 地址绑定

前面讲过计算机的网卡有MAC，且全球唯一。要设置交换机的端口和计算机进行绑定，你只需要设置交换机的端口和计算机的 MAC 地址进行绑定即可。

打开随书光盘中第 7 章练习“03 交换机端口和计算机绑定.pkt”，网络拓扑如图 7-11 所示，计算机和 DHCP 服务器的 IP 地址已经配置完成。你需要设置交换机的端口和现在的计算机的 MAC 地址进行绑定。



▲图 7-11 网络拓扑

（1）使用 PC0 ping PC1、PC2 和 DHCP，这样交换机就能构造 MAC 地址表。

（2）查看交换机的 MAC 地址表。

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

```
   1     0000.0c7c.7e49     DYNAMIC     Fa0/4  --DYNAMIC 表示是动态学习到的
   1     0001.63c6.e338     DYNAMIC            Fa0/2
   1     0090.0cd7.65c8      DYNAMIC           Fa0/1
   1     00d0.ffce.0eb4      DYNAMIC           Fa0/3
```

（3）将上面显示的 MAC 地址和交换机端口进行绑定。

```
Switch#config t    --进入全局配置模式
Switch (config) #interface range fastEthernet 0/1～4
                          --这种方式可以配置接口 1～4
Switch (config-if-range) #switchport mode access
                          --将交换机端口设置为 access，明确该端口连接的是计算机
Switch (config-if-range) #switchport port-security
                          --在交换机端口启用安全
Switch (config-if-range) #switchport port-security violation shutdown
                          --违反安全规则后禁用
Switch (config-if-range) #switchport port-security mac-address sticky
                         --将上面的动态的 MAC 地址和端口进行绑定
```

以上命令必须依次执行，顺序颠倒会出现错误。

（4）再次查看 MAC 地址表。

```
Switch#show mac-address-table。
        Mac Address Table
-------------------------------------------
Vlan    Mac Address        Type       Ports
----   -----------       --------    -----
   1     0000.0c7c.7e49    STATIC      Fa0/4       --可以看到类型变为 STATIC
   1     0001.63c6.e338    STATIC      Fa0/2       --可以看到类型变为 STATIC
   1     0090.0cd7.65c8    STATIC      Fa0/1       --可以看到类型变为 STATIC
   1     00d0.ffce.0eb4    STATIC       Fa0/3      --可以看到类型变为 STATIC
```

可以看到 FastEthernet 0/1～4 对应的 MAC 地址为 STATIC，不会过期，且不再动态学习。如果 MAC 地址表为空，请重复步骤①，因为 DYNAMIC 的条目过一段时间就删除了。

（5）查看配置。

```
Switch#show running-config
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.0CD7.65C8
```

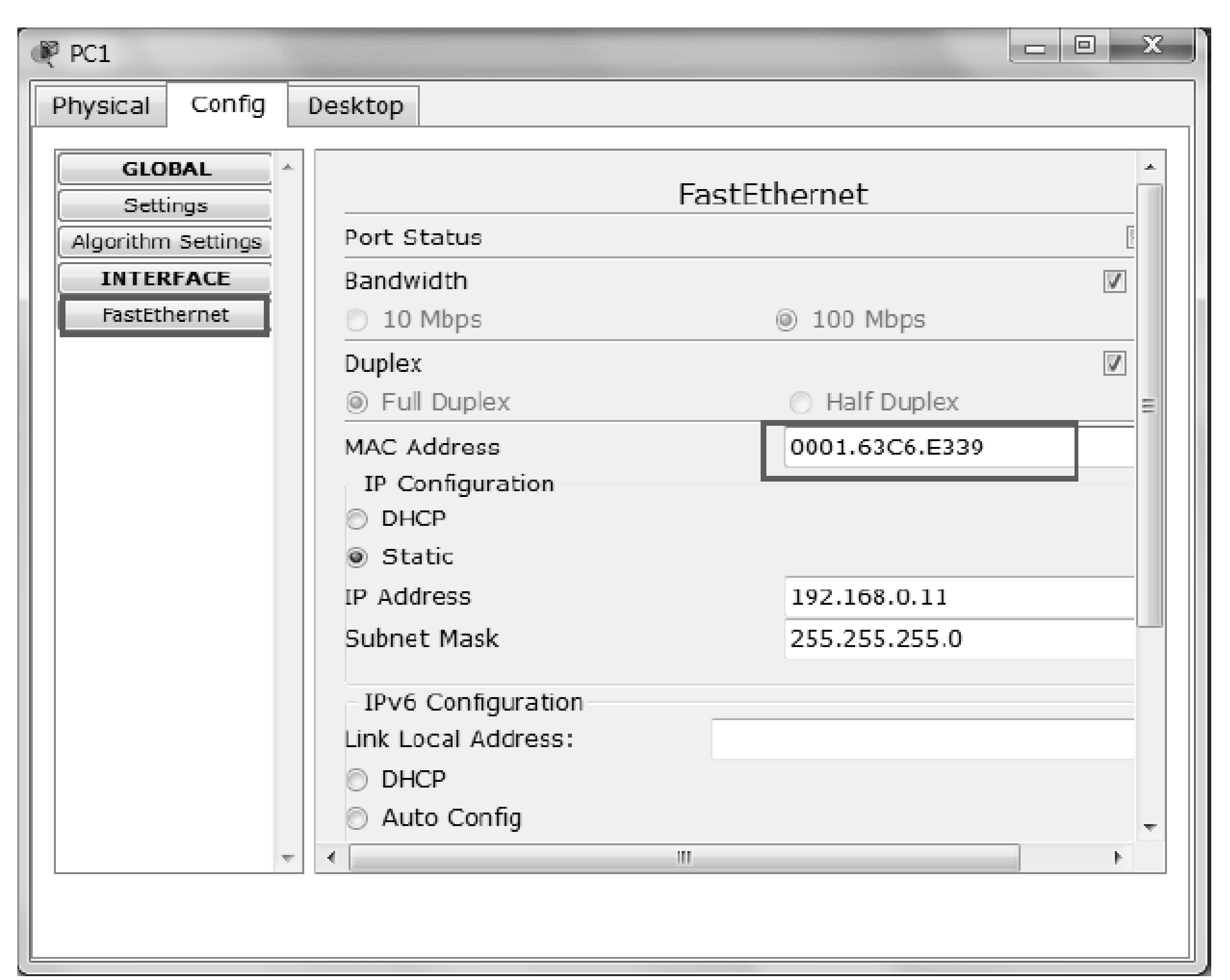
你能看到 Interface FastEthernet 0/1～4 的端口安全设置。

（6）保存配置。

```
Switch#copy running-config startup-config
                --将以上配置保存，交换机重启，端口安全设置依旧在。
```

（7）验证违反后端口被自动禁用。

如图 7-12 所示，更改 PC1 网卡的 MAC 地址，将 0001.63C6.E338 更改为 0001.63C6.E339，你会立即发现交换机上连接 PC1 的端口变红，说明该接口已经被禁用。使用 PC0 ping PC1 的 IP 地址，不通。



▲图 7-12　更改 MAC 地址

如果你不嫌麻烦，可以一个一个地对每一个交换机端口进行和 MAC 地址的绑定。

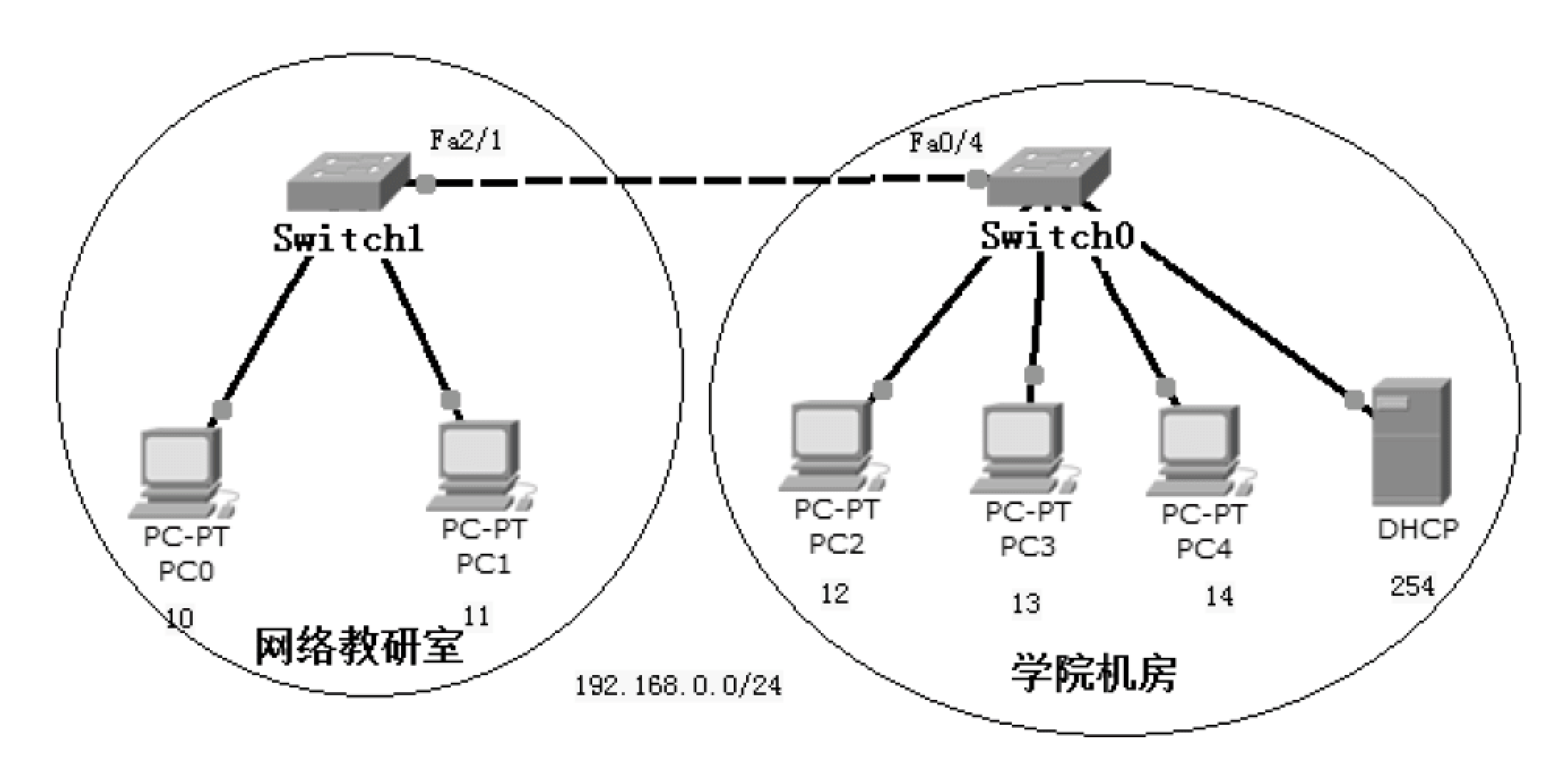
```
Switch（config）#interface fastEthernet 0/2
Switch（config-if）#switchport mode access
Switch（config-if）#switchport port-security
Switch（config-if）#switchport port-security violation shutdown
Switch（config-if）#switchport port-security mac-address 0001.63C6.E338
```

以下命令关闭交换机端口安全设置（在 Packet Tracer 软件模拟的交换机上，需要关闭 Packet Tracer，保存，再次打开，设置生效）。

```
Switch（config-if）#no switchport port-security
```

7.4.2　控制端口连接计算机的数量

在交换机的端口上还可以设置某个端口能够连接的计算机数量。打开随书光盘中第 7 章练习“04 控制端口连接计算机的数量.pkt”，网络拓扑如图 7-13 所示，河北师大软件学院网络教研室通过交换机 Switch1 和学院机房的交换机 Switch0 的 Fa0/4 相连。网络教研室目前只有两台计算机，学院的 IT 管理员不希望网络教研室随便在 Switch1 上连接更多的计算机。可以设置 Switch0 的 Fa0/4 接口的安全来实现。



▲图 7-13 网络拓扑

（1）在交换机 Switch0 上的设置：配置端口安全。

```
Switch>en
Switch#config t
Switch（config）#interface fastEthernet 0/4
Switch（config-if）#switchport mode access
Switch（config-if）#switchport port-security
Switch（config-if）#switchport port-security violation shutdown
Switch（config-if）#switchport port-security maximum 2
```

（2）你可以将 PC2 的网线连接到 Switch1，然后使用 PC3 ping PC0、PC1 和 PC2。可以看到 Switch0 的 F0/4 端口关闭。

7.5 VLAN

交换机虽然比网桥和集线器的性能高，并且独享端口带宽，每一个端口是一个冲突域，但是使用交换机组建的网络在同一网段中的计算机数量却不能太多，为什么呢？

前面讲过交换机隔绝冲突域，但是如果网络中的计算机发送广播帧，即目标 MAC 地址为 FFFF.FFFF.FFFF.FFFF 的交换机将这类帧发送到所有端口。同一网段内计算机数量增多，发送广播的帧也就增多，将会消耗更多的带宽。如果某个计算机中了 ARP 病毒仍在网上大量发送广播，将会造成网络堵塞；或者有 MAC 地址欺骗的病毒，将会影响同一网段内所有计算机的网络互连。

出于安全考虑，公司的网络规划有可能将同一个部门的计算机放置到一个网段，或安全性要求一致的计算机放置到一个网段，而不是按照计算机的物理位置划分网段。比如，将能够访问 Internet 的计算机放置到一个网段，然后在防火墙上进行配置，只允许该网段能够访问 Internet。

基于以上原因，我们可以使用交换机按部门灵活地划分网段，而不用考虑物理位置，这

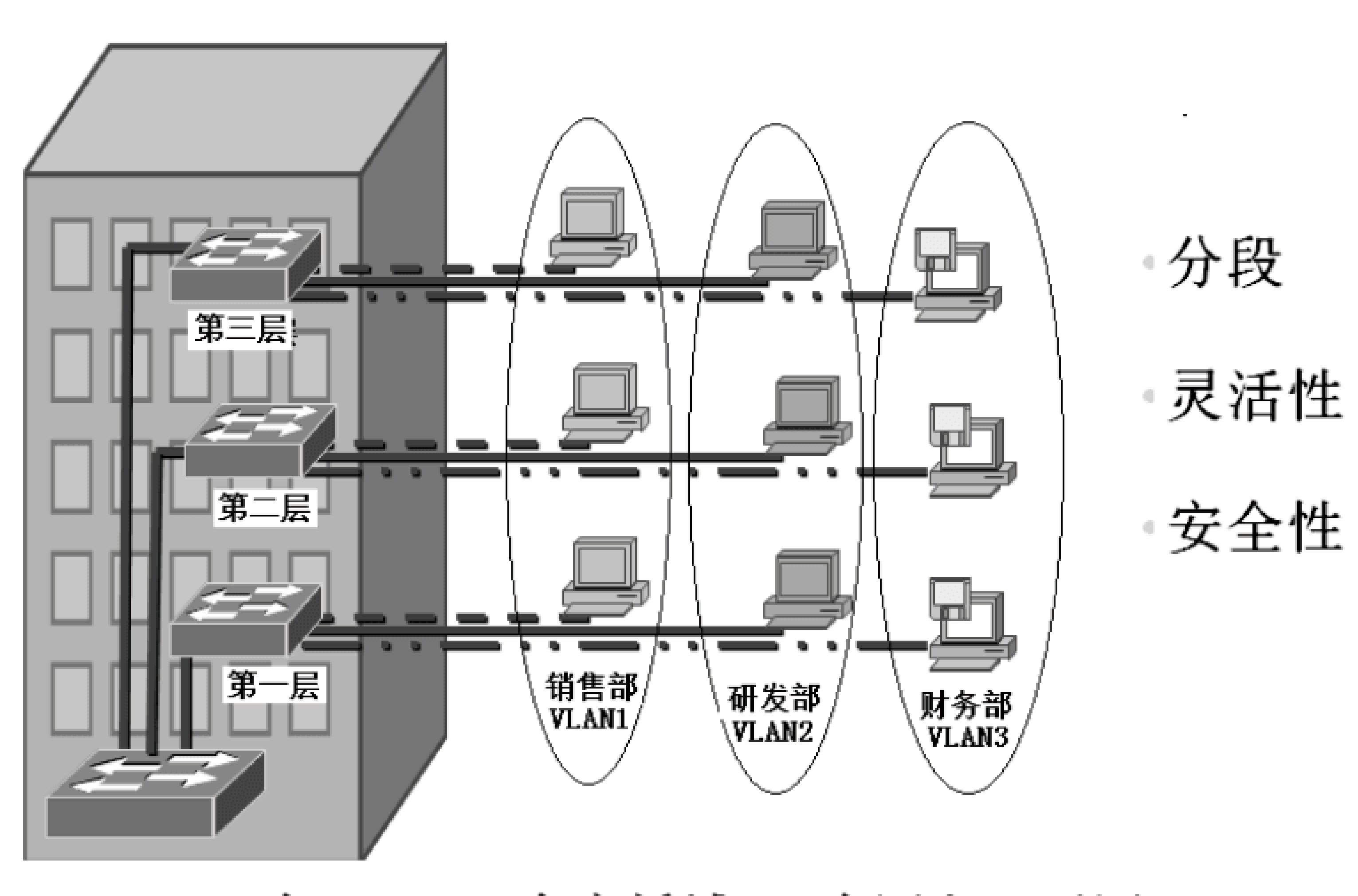
就是下面要讲解的 VLAN 技术。

7.5.1 什么是 VLAN

VLAN（Virtual Local Area Network，虚拟局域网）技术的出现，主要是为了解决交换机在进行局域网互连时无法限制广播的问题。这种技术可以把一个 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，因此，广播报文被限制在一个 VLAN 内。VLAN 是一种将局域网设备从逻辑上划分成一个个网段而不用考虑同一个 LAN 是否在同一个交换机上。

如图 7-14 所示，公司的办公大楼在第一层、第二层和第三层放置了交换机，这三个交换机为接入层交换机，通过汇聚层交换机连接。公司的销售部、研发部和财务部的计算机在每一层都有。从安全和控制网络广播方面考虑，可以为每一个部门创建一个 VLAN。在交换机上不同的 VLAN 使用数字标识，你可以将销售部的计算机指定到 VLAN 1，为研发部创建 VLAN 2，为财务部创建 VLAN 3。

一个 VLAN 就是一个广播域，同一个 VLAN 中的计算机 IP 地址在同一个网段。



▲图 7-14　VLAN 示意图

1. VLAN 的优点

- 广播风暴防范

限制网络上的广播，将网络划分为多个 VLAN 可减少参与广播风暴的设备数量。LAN 分段可以防止广播风暴波及整个网络。VLAN 可以提供建立防火墙的机制，防止交换网络的过量广播。使用 VLAN，可以将某个交换端口或用户赋于某一个特定的 VLAN 组，该 VLAN 组可以在一个交换网中或跨接多个交换机，在一个 VLAN 中的广播不会送到 VLAN 之外。同样，相邻的端口不会收到其他 VLAN 产生的广播，这样可以减少广播流量，释放带宽给用户应用，减少广播的产生。

- 安全

增强局域网的安全性，含有敏感数据的用户组可与网络的其余部分隔离，从而降低泄露机密信息的可能性。不同 VLAN 内的报文在传输时是相互隔离的，即一个 VLAN 内的用户不能和其他 VLAN 内的用户直接通信。如果不同 VLAN 间要进行通信，则需要通过路由器或三层交换机等三层设备。

2．创建 VLAN 的条件

VLAN 是建立在物理网络基础上的一种逻辑子网，因此建立 VLAN 需要相应的支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，需要路由的支持，这时就需要增加路由设备——要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

7.5.2 创建和管理 VLAN

打开随书光盘中第 7 章练习“05 创建和管理 VLAN.pkt”，网络拓扑如图 7-15 所示，网络中的计算机已经配置好了 IP 地址，交换机的所有接口默认都属于 VLAN 1。PC0 和 PC1 分别连接到交换机的 Fa0/1 和 Fa0/2 接口，PC3 和 PC4 分别连接在交换机的 Fa0/13 和 Fa0/14。

本实验将会查看交换机上的 VLAN，端口所属的 VLAN，创建 VLAN 2，将 13-24 端口指定到 VLAN 2，然后测试 PC0 和 PC1 和 PC2 是否能通信。删除 VLAN2，查看属于 VLAN 2 的端口。

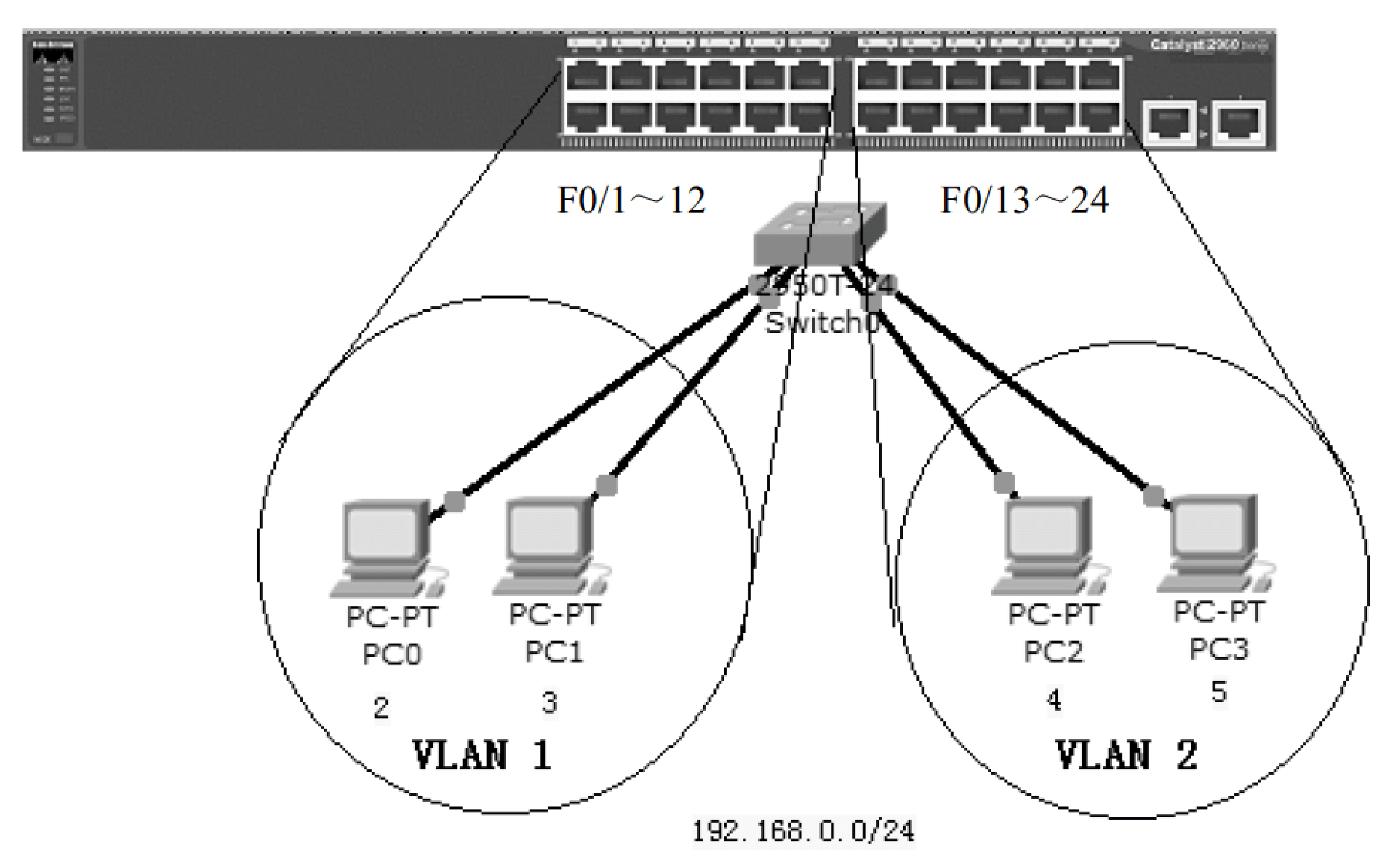


图 7-15 创建和管理 VLAN

操作步骤如下。

（1）查看交换机的 VLAN，如图 7-16 所示。

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig1/1, Gig1/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

▲图 7-16　显示 VLAN

在交换机上运行 show vlan，可以看到所有的接口都在 VLAN 1，VLAN 1 是默认 VLAN，不能删除，也不需要创建。

（2）使用 PC0 ping PC1、PC2 和 PC3，将发现都能通，在同一个 VLAN 的计算机 IP 地址在一个网段就能通信。

（3）创建 VLAN 2，将 Fa0/13～24 端口指定到 VLAN 2。

```
Switch>en
Switch#config t
Switch（config）#vlan 2  --创建 VLAN 2，就这么简单，删除 VLAN 2 只需 no vlan 2
Switch（config-vlan）#exit
Switch（config）#interface range fastEthernet 0/13-24
Switch（config-if-range）#switchport mode access
                                  --access 指定这些接口为访问接口
Switch（config-if-range）#switchport access vlan 2
                                  --将这些接口指定到 VLAN 2
```

后面会为大家介绍什么是访问接口和干道接口。

（4）查看 VLAN，如图 7-17 所示。

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Gig1/1, Gig1/2
2    VLAN0002                         active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

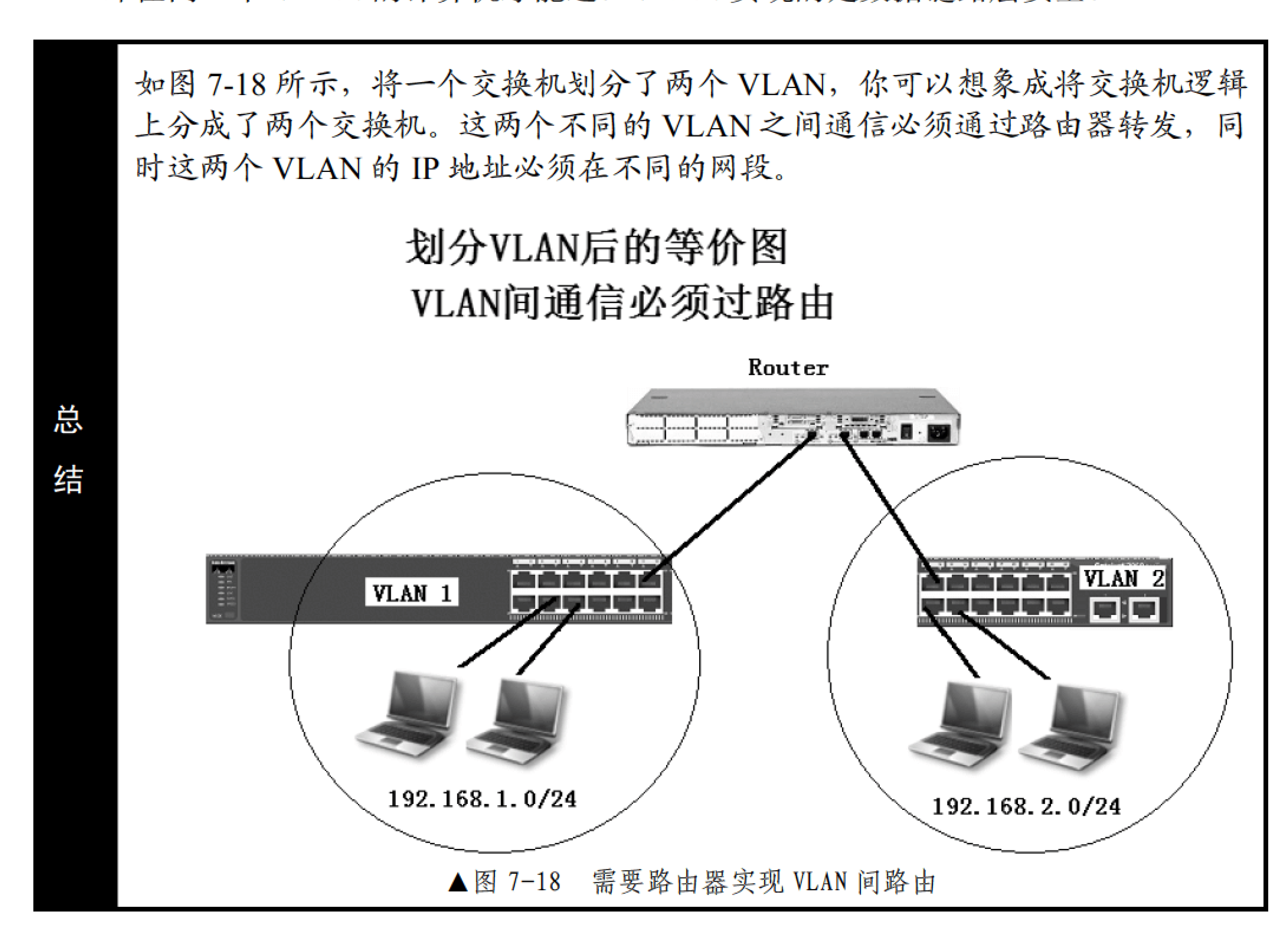
▲图 7-17　查看 VLAN

可以看到创建的 VLAN 2，以及 VLAN 2 的接口。

（5）现在使用 PC0 ping PC1、PC2 和 PC3，发现只能 ping 通 PC1。PC2 能够 ping 通 PC3。即在同一个 VLAN 的计算机才能通。VLAN 实现的是数据链路层安全。

总结

如图 7-18 所示，将一个交换机划分了两个 VLAN，你可以想象成将交换机逻辑上分成了两个交换机。这两个不同的 VLAN 之间通信必须通过路由器转发，同时这两个 VLAN 的 IP 地址必须在不同的网段。



▲图 7-18 需要路由器实现 VLAN 间路由

（6）删除 VLAN 2。

```
Switch (config) #no vlan 2      --删除 VLAN 2
```

（7）查看 VLAN。

```
Switch#show vlan
```

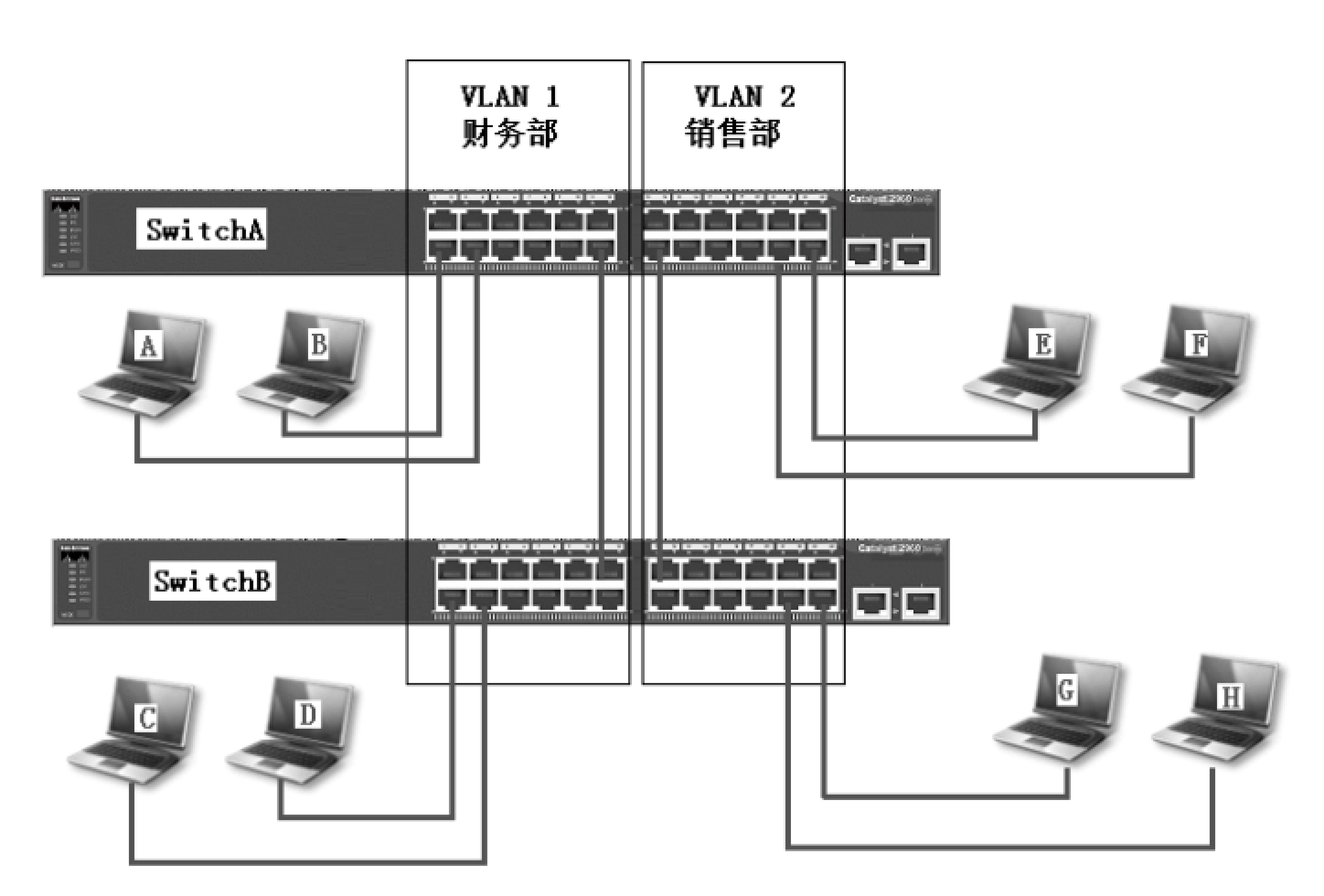
可以看到，删除 VLAN 2 后， VLAN 2 的端口不属于任何 VLAN，这些端口被禁用，你需要明确指定这些端口所属的 VLAN，这些端口才会被启用。

7.5.3 跨交换机的 VLAN

以上讲的是将一个交换机划分为两个 VLAN。如图 7-19 所示，某公司有两个部门，财务部和销售部，分别接在两个交换机 SwitchA 和 SwitchB 上。如果将财务部的计算机规划到 VLAN 1，将销售部的计算机规划到 VLAN2，如何实现呢？

在两个交换机上分别创建 VLAN2，将连接销售部计算机的端口指定到 VLAN2。将连接财务部计算机的端口指定到 VLAN1。为了确保两个交换机上的 VLAN1 能够直接通信，可以使用一根网线将两个交换机属于 VLAN1 的端口连接，使用另一根网线将两个交换机属于 VLAN2 的端口连接。这样，VLAN1 的计算机 A、B、C、D 就属于同一个逻辑网段了，销售部的计算机 E、F、G、H 就属于另一个逻辑网段了。

按照上面的方法，如果有 10 个 VLAN 跨这两个交换机，每一个 VLAN 使用一根网线连接两个交换机，就太浪费交换机端口和网线了。有没有更好的方法呢？有！那就是使用干道链路。下面将介绍什么是干道链路。



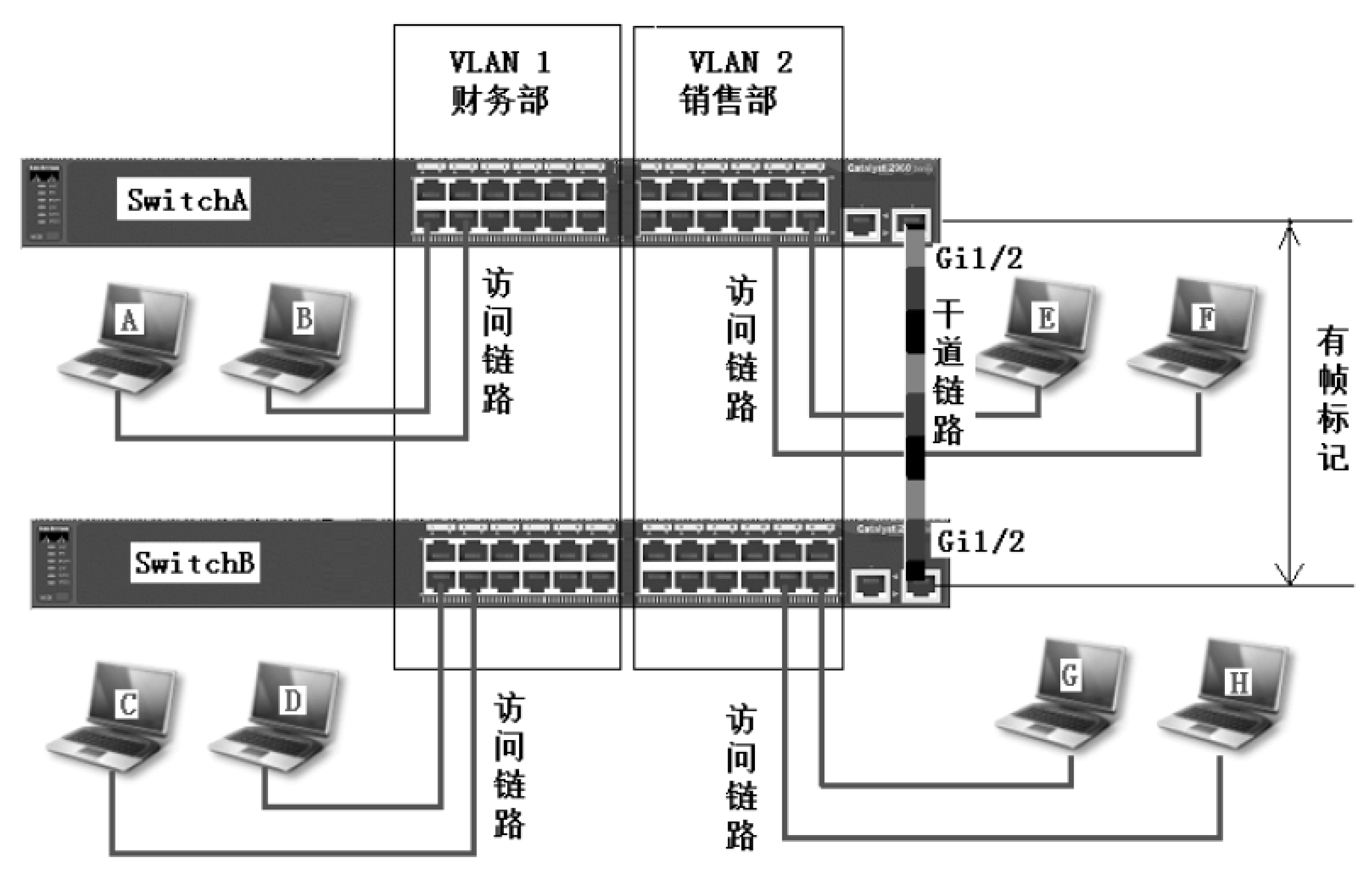
▲图 7-19　跨交换机的 VLAN

交换机的端口有以下两种类型。

- 访问端口：访问端口只能属于某一个 VLAN，它只能承载某一个 VLAN 的流量。连接访问端口的链路称为访问链路。
- 中继端口：中继端口能够同时承载多个 VLAN 的流量，连接中继端口的链路称为干道链路。数据帧进入干道链路时需要添加帧标记（或称 VLAN ID），离开干道链路时去掉帧标记，这个过程对计算机来说是透明的。

现在介绍数据帧通过干道链路添加帧标记的意义：通过干道的数据帧用来标明该帧来自哪个 VLAN。

如图 7-20 所示，计算机 A 发送一个广播帧，SwitchA 知道计算机 A 属于 VLAN1，就将该广播发送到 VLAN1 的所有端口。这个广播帧还会通过干道链路发送到 SwitchB，SwitchB 需要将该广播帧发送到 SwitchB 的 VLAN1 的所有端口。问题是 SwitchB 如何知道该广播帧来自哪个 VLAN？这就需要 SwitchA 将来自 VLAN1 的数据帧添加一个帧标记标明其所属的 VLAN，当 SwitchB 接收后就知道应该将该帧广播到哪个 VLAN。这个数据帧只要离开干道链路就去掉帧标记。在访问链路上是没有帧标记的。



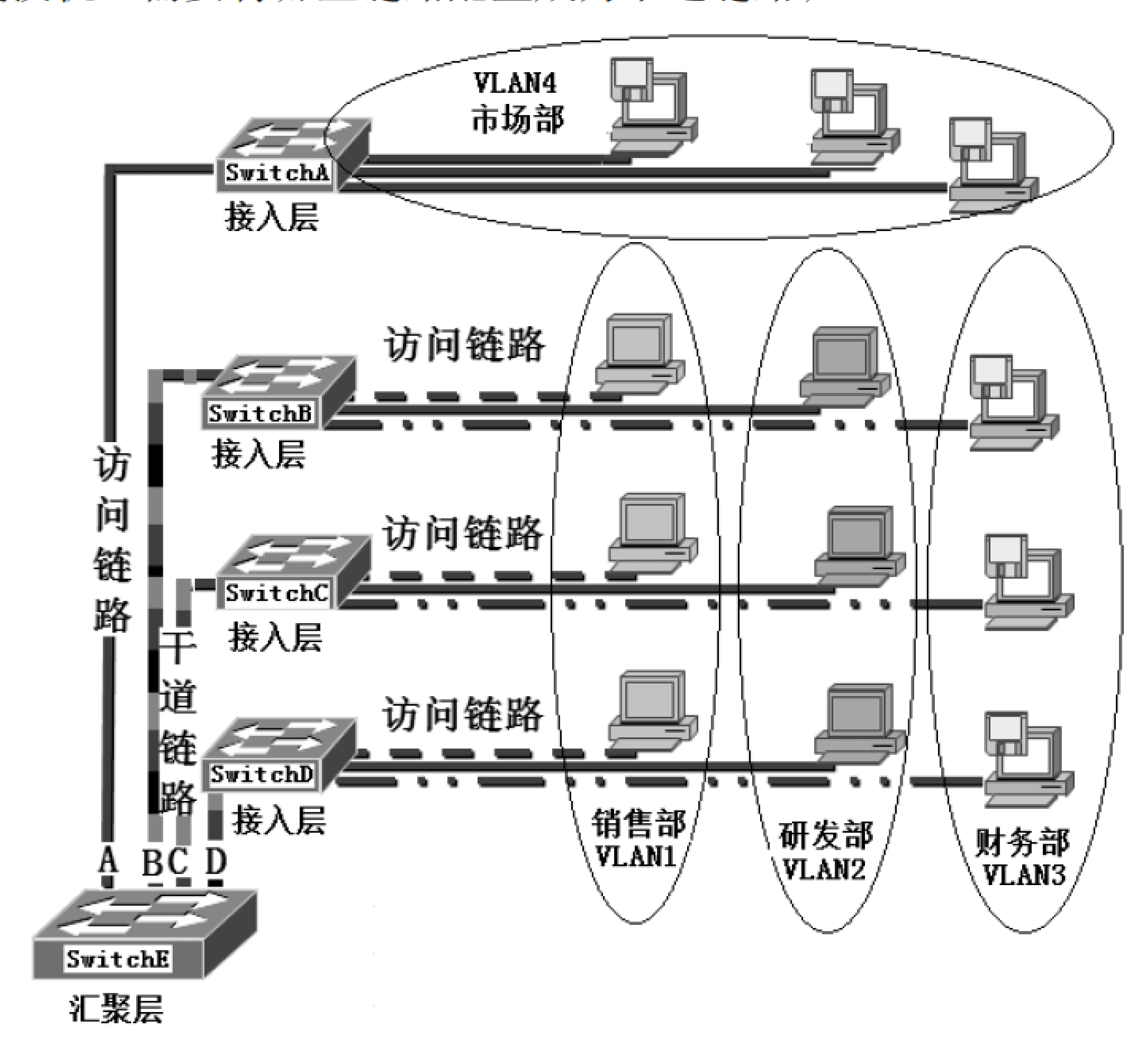
▲图 7-20　通过干道链路连接多个 VLAN

为了说明方便给大家举例广播帧通过干道链路添加帧标记，其实非广播帧通过干道链路

同样可以添加帧标记。

这样不管有多少个 VLAN 跨这两个交换机，只需一条干道链路即可。

如图 7-21 所示，接入层交换机 SwitchA、SwitchB、SwitchC、SwitchD 于汇聚层交换机 SwitchE 处连接。市场部计算机都连接到 SwitchA，属于 VLAN 4。销售部和研发部以及财务部的计算机分别属于 VLAN1、VLAN2 和 VLAN3，这三个 VLAN 跨 SwitchB、SwitchC 和 SwitchD 三个交换机，需要将哪些链路配置成为干道链路呢？



▲图 7-21　需要配置为干道的链路

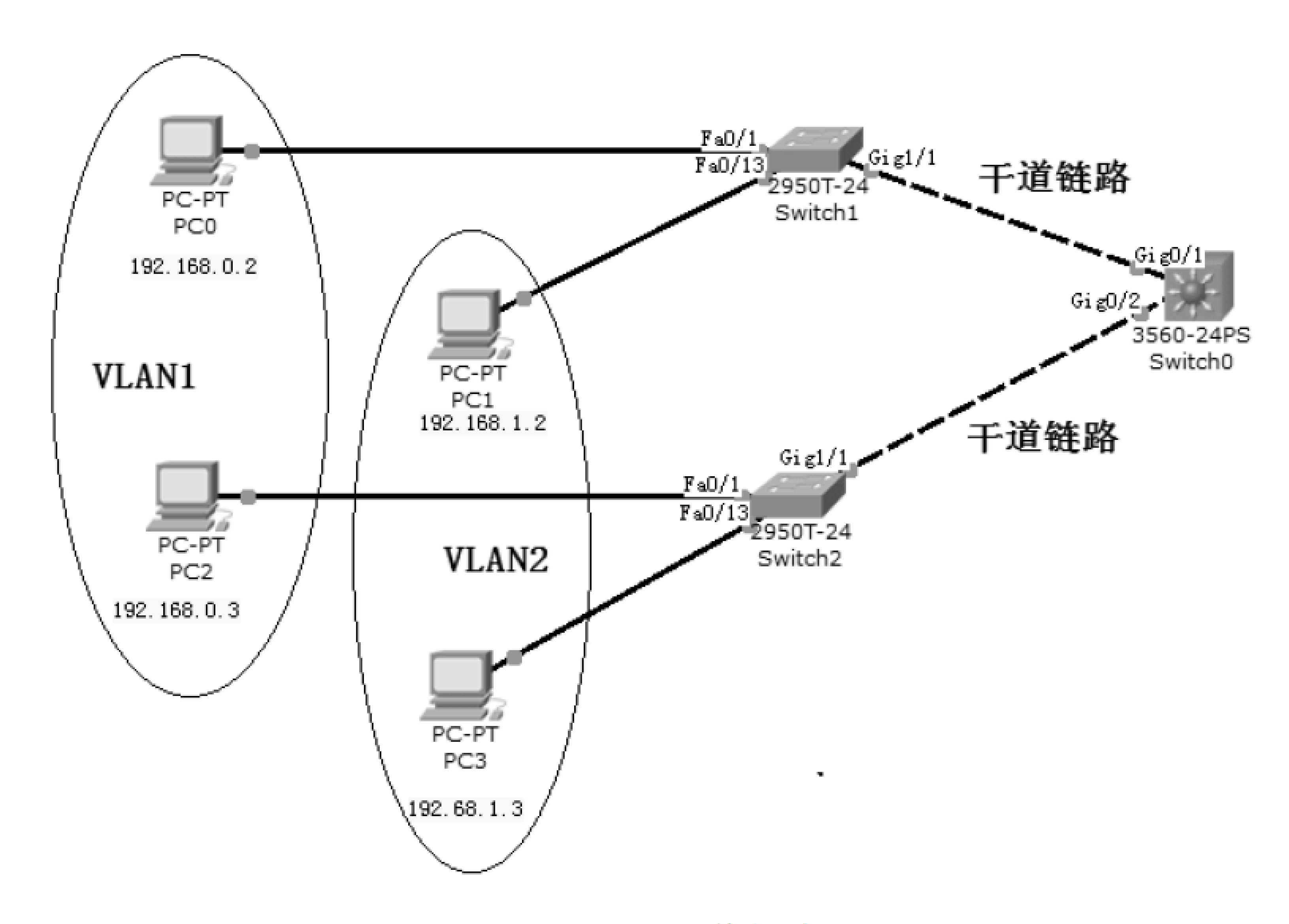
传递多个 VLAN 数据的链路需要配置成干道链路，因此 SwitchB、SwitchC、SwitchD 与 SwitchE 连接的链路需要配置为干道，而 SwitchA 上连接的是同一个 VLAN 的计算机，因此 SwitchA 与 SwitchE 之间的连接可以使用访问链路连接。

总结	在交换机组建的网络中，如果需要多个 VLAN 通过的链路则需要配置为干道链路。如果链路上只需要单一 VLAN 的数据通过则可以配置为访问链路。

7.5.4　配置干道链路

打开随书光盘中第 7 章练习“06 配置干道链路.pkt”，如图 7-22 所示，网络中的交换机 Switch1、Switch2 是接入层交换机，Switch0 是汇聚层交换机。VLAN1 和 VLAN2 跨三个交换机。

现在你需要在 Switch1、Switch2、Switch0 上创建 VLAN2，前两个交换机将 Fa0/13～24 端口指定到 VLAN2。将连接汇聚层交换机的端口指定为干道链路。验证 VLAN1 的两个计算机 PC0 和 PC2 能够通信，VLAN2 的两个计算机 PC1 和 PC3 能够相互通信。



▲图 7-22 网络拓扑

操作步骤如下。

（1）在 Switch1 和 Switch2 上，创建 VLAN 2，配置干道端口。

```
Switch>en
Switch#config t
Switch (config) #vlan 2  --创建 VLAN2
Switch (config-vlan) #ex
Switch (config) #interface range fastEthernet 0/13 - 24 --进入接口配置模式
Switch (config-if-range) #switchport mode access        --将接口设置为访问接口
Switch (config-if-range) #switchport access vlan 2      --将接口指定到 VLAN2
Switch (config-if-range) #ex
Switch (config) #interface gigabitEthernet 1/1
Switch (config-if) #switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally
Switch (config-if) #switchport mode trunk          --将接口指定为干道接口
```

（2）在 Switch0 上，创建 VLAN 2，配置干道链路。

```
Switch>en
Switch#config t
Switch (config) #vlan 2 --创建 VLAN2
Switch (config-vlan) #ex
Switch (config) #interface range gigabitEthernet 0/1 - 2 --进入接口配置模式
Switch (config-if-range) #switchport trunk encapsulation dot1q
```

```
                                    --指定干道链路 VLAN 标识方法
Switch (config-if-range) #switchport mode trunk  --将接口指定为干道接口
```

（3）在 PC0 上 ping PC2。

```
PC>ping 192.168.0.3
```

（4）在 PC1 上 Ping PC3。

```
PC>ping 192.168.1.3
```

> **注意**
> 只有 FastEthernet 和 gigabitEthernet 接口支持干道。
> 必须在 Switch0 上创建 VLAN2，虽然没有 VLAN2 的计算机直接连接到该交换机。
> 在 Switch0 上将接口配置为干道前，必须指定干道链路 VLAN 的标识方法。

7.5.5 帧标记

关于中继端口的另一件事情是，它们将同时支持标记的和非标记的流量（我们将在下面讨论采用 802.1Q 的中继）。对于所有非标记的流量将要穿越的 VLAN 中继端口将被分配一个默认的端口 VLAN ID（PVID）。 这种 VLAN 也称为本机（native）VLAN，默认时，它始终是 VLAN 1（但可以改为任何 VLAN 号）。

类似地，任何带 NULL（没有分配的）VLAN ID 的标记或非标记流量，都假定属于有端口默认 PVID 的 VLAN（同样，默认时为 VLAN1）。其 VLAN ID 等于外出端口默认 PVID 的数据包将作为非标记流量发送，且只能与 VLAN1 中的主机或设备进行通信。其他所有的 VLAN 流量必须用 VLAN 标记发送，以便在与此标记相对应的特定 VLAN 中通信。

VLAN 的识别方法

VLAN 的识别是指当帧通过干道链路时，交换机跟踪帧所属 VLAN 的方式。它指的是交换机怎样识别哪一个帧属于哪一个 VLAN，下面是一些实现中继的方法。

- 交换机间链路

交换机间链路（Inter-Switch Link，ISL）是一种在以太网帧上显式地标记 VLAN 信息的方法。通过一种外部封装方法（ISL），这种标记信息允许 VLAN 在干道链路上实现多路复用，从而允许交换机在中继链路上识别出帧的 VLAN 成员关系。

通过运行 ISL，可以将多台交换机互联起来，当流量在交换机之间的中继链路上传送时，仍然维持 VLAN 信息。ISL 在第 2 层起作用，并用新的报头和循环冗余校验（CRC）对数据帧进行封装。

要注意的是，这是 Cisco 交换机专用的方法，它只用于快速以太网和吉比特以太网链路。ISL 路由的用途相当广泛，可以用在交换机端口、路由器接口和服务器接口卡上。

- IEEE 802.1Q

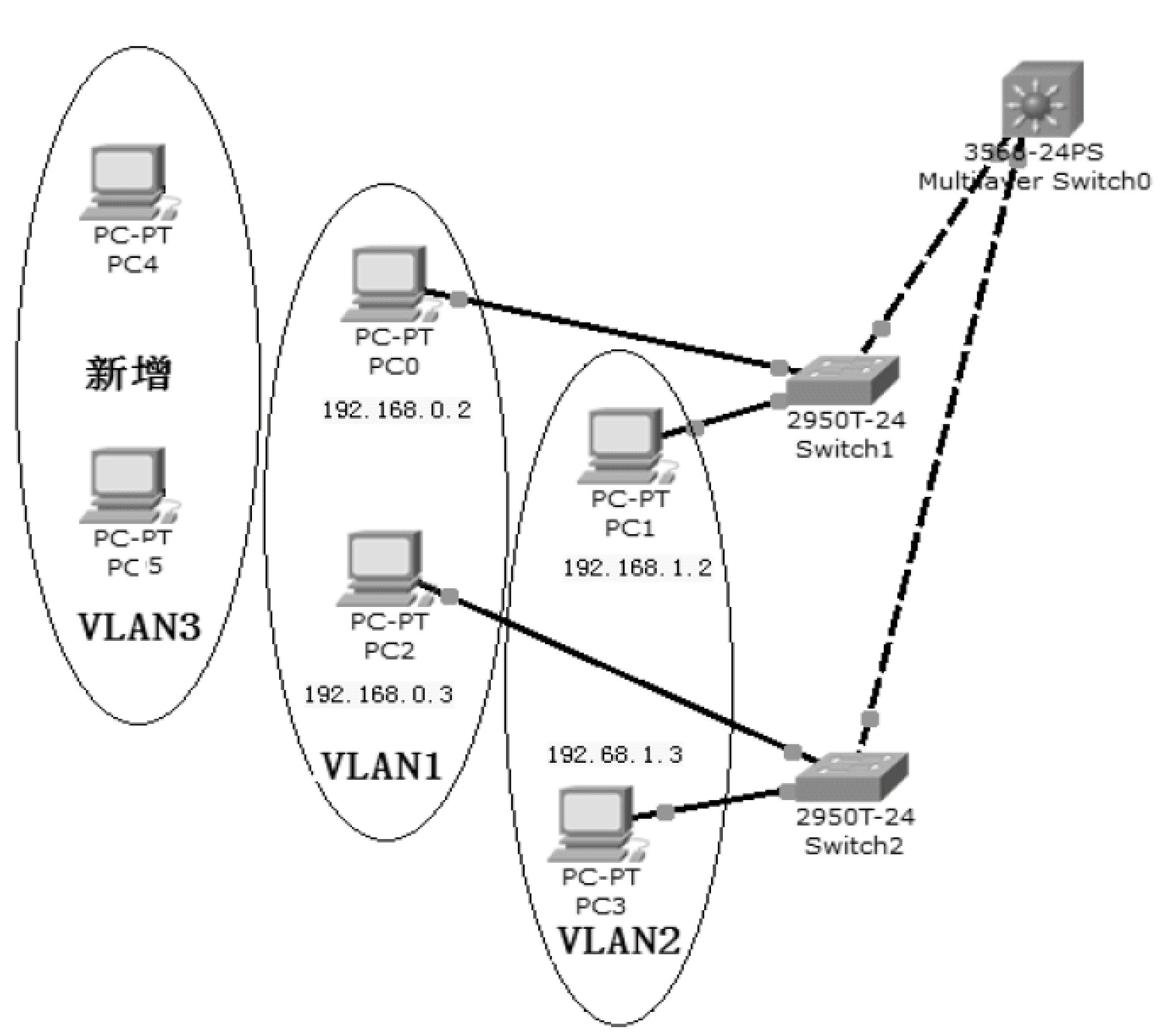
IEEE 802.1Q 是由 IEEE 创建的，作为帧标记的标准方法，它实际上是在帧中插入一个字段，以标识 VLAN。如果你正在 Cisco 的交换式链路和不同品牌的交换机之间设置中继链路，就不得不使用 802.1Q，以便让中继链路起作用。

它的原理是这样的：首先指定准备采用 802.1Q 封装来实现中继的每个端口，必须为端口分配特定的 VLAN ID，使它们成为本机 VLAN，以便让它们通信。属于同一个中继链路的端口所创建的工作组就成为本机 VLAN，每个端口用反映其本机 VLAN 的标识号作为标记，默认时为 VLAN1。本机 VLAN 允许中继链路传送所接收到的没有任何 VLAN 标识或帧标记的信息。

2960 系列只支持 IEEE 802.1Q 中继协议，但 3560 系列能支持 ISL 和 IEEE 两种方法。

7.5.6 VLAN 干道协议（VTP）

如图 7-23 所示，Switch1、Switch2 通过干道和 Switch0 连接。如果网络中需要新增加一个 VLAN3，你需要在 Switch1、Switch2 以及 Switch0 上创建 VLAN3；如果网络中需要将 VLAN 2 删除，你需要在 Switch1、Switch2 以及 Switch0 上删除 VLAN 2。有没有简单的方法管理 VLAN 的添加和删除呢？



▲图 7-23　VTP 协议的作用示意图

有！那就是配置 VLAN 干道协议（VLAN Trunk Protocol，VTP），使用 VTP 能够在干道链路上通告 VLAN 添加或删除的消息。需要配置以下参数，才能实现交换机间 VLAN 信息共享。

```
Switch（config）#vtp domain todd     --必须有相同的 VTP 域名
Switch（config）#vtp password aaa    --必须有相同的密码，为了安全考虑最好设置密码
Switch(config)#vtp mode ?      --可以看到 VTP 模式有 Client、Server 和 Transparent
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
```

如果将交换机的 VTP 模式设置为 Server，你能够在该交换机上添加、删除 VLAN，这些更改将会通过 VTP 协议通告给同一个 VTP 中的其他交换机。一个 VTP 域中最少应该有 1 个交换机作为 Server。在 VTP 服务器模式下，VLAN 的配置保存在 NVRAM 中。

如果将交换机的 VTP 模式设置为 Client，该交换机从 VTP 服务器接收 VLAN 信息，同时也发送和接收更新。你不能在这些交换机上添加或删除 VLAN。VLAN 信息不存储在 NVRAM 中，一旦重启交换机，就需要重新从 VTP 的服务器上学习 VLAN 信息。

如果将交换机的 VTP 模式设置为 Transparent，能够通过干道链路通告 VTP 信息，但不会修改自己的 VLAN 信息。

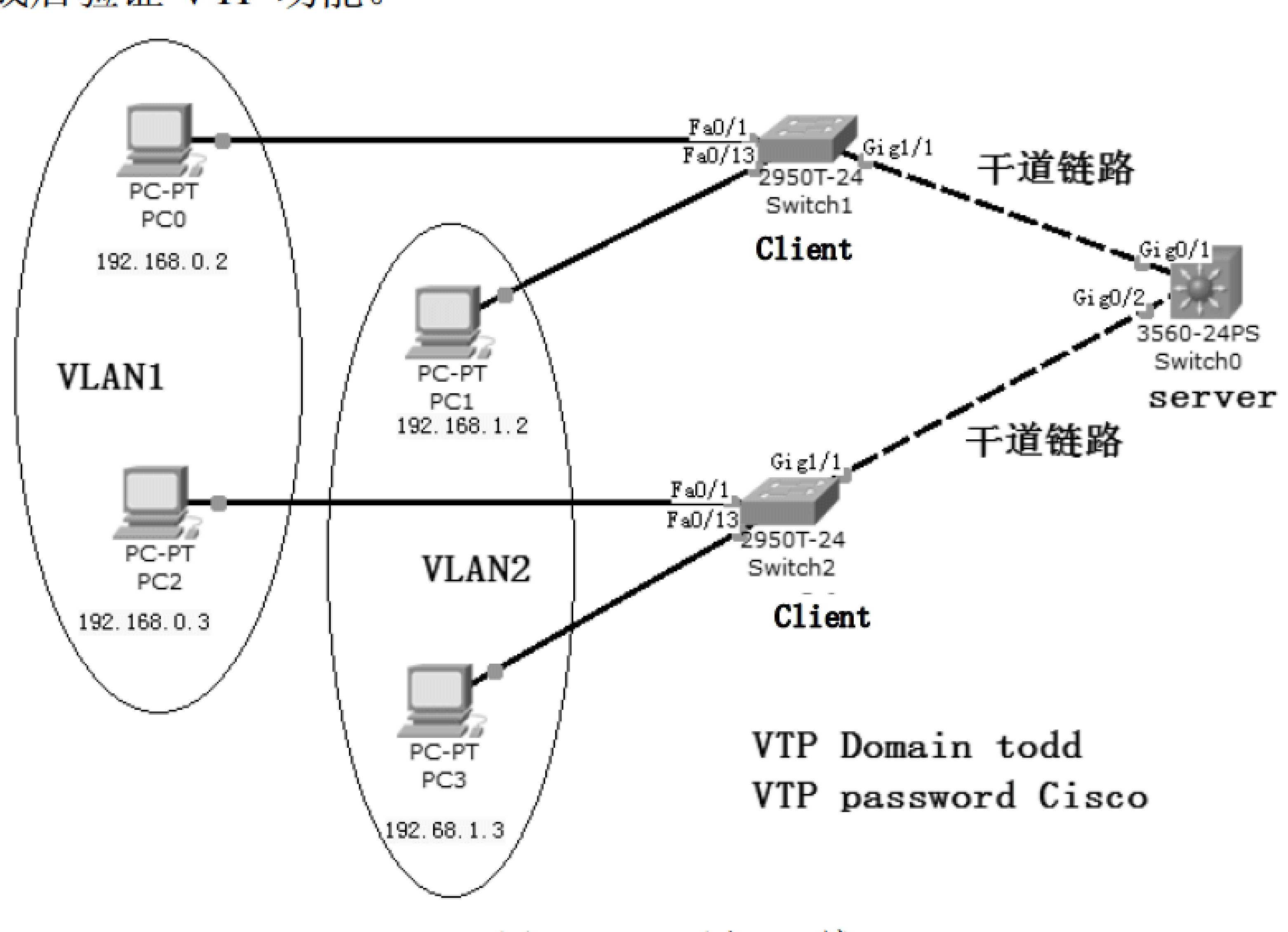
7.5.7 配置 VTP 域

打开随书光盘中第 7 章练习“07 配置 VTP 域.pkt”，交换机间连接已经配置为干道链路，网络拓扑如图 7-24 所示。

你需要配置这三个交换机在同一个 VTP 域“todd”，VTP 密码为“Cisco”。

Switch0 作为 VTP 的 Server，Switch1 和 Switch2 作为 VTP 的 Client。

配置完成后验证 VTP 功能。



▲图 7-24 配置 VTP 域

操作步骤如下。

（1）在 Switch1 和 Switch2 上，配置 VTP 域名、密码和模式。

```
Switch (config) #vt
Switch (config) #vtp domain todd
Switch (config) #vtp password Cisco
Switch (config) #vtp mode client
```

（2）在 Switch0 上，配置 VTP 域名、密码和模式。

```
Switch>en
```

```
Switch#config t
Switch (config) #vtp domain todd
Setting device VLAN database password to Cisco
Switch (config) #vtp mode server
```

（3）在 Switch0 上创建 VLAN 40。

```
Switch (config) #vlan 40
```

（4）在 Switch1 和 Switch2 上查看 VLAN。

```
Switch#show vlan
VLAN Name                             Status    Ports
---------------------------- ------------ -------------------------------
1    default                        active      Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Gig1/2
2    VLAN0002                       active      Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
40   VLAN0040                       active
```

可以看到，在 Switch0 上创建的 VLAN，在 Switch1 和 Switch2 上都能看到。

（5）在 Switch1 上删除 VLAN 40，创建 VLAN 30。

```
Switch (config) #no vlan 40
VTP VLAN configuration not allowed when device is in CLIENT mode.
Switch (config) #vlan 30
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

提示 在 Client 模式设备上不能删除 VLAN，也不能创建 VLAN。

（6）你可以更改 Switch1 的 VTP 模式为 Server，即可在该设备上创建和删除 VLAN。

```
Switch (config) #vtp mode server
```

（7）在 Switch0 上查看 VTP 配置

```
Switch#show vtp status
VTP Version                      --2
Configuration Revision           --10
Maximum VLANs supported locally --1005
Number of existing VLANs         --7
VTP Operating Mode               --Server
```

```
VTP Domain Name                   --todd
VTP Pruning Mode                  --Disabled
VTP V2 Mode                       --Disabled
VTP Traps Generation              --Disabled
MD5 digest                        --0xE2 0xB1 0xA5 0x30 0xE5 0x68 0xD5 0xA4
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

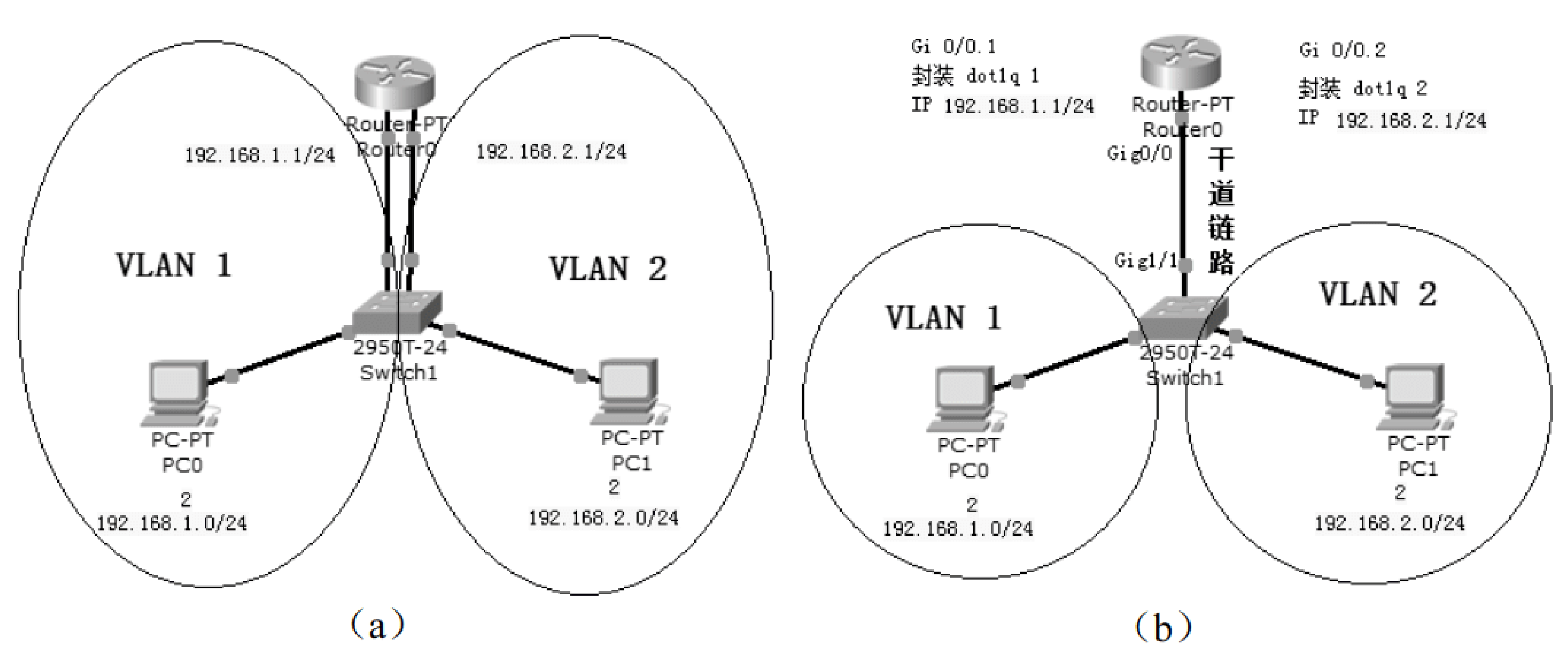
总结 将交换机设置为同一个 VTP 域，一个 VTP 域最少有一个 VTP Server，在 Server 上可以方便地管理交换机中 VLAN 的添加或删除。你需要在每一个交换机上将交换机的端口指定到特定 VLAN，这一点没有办法统一管理。

7.6 配置 VLAN 间路由

VLAN 是建立在物理网络基础上的一种逻辑子网，因此建立 VLAN 需要相应的支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，需要路由的支持，这时就需要增加路由设备——要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

7.6.1 单臂路由器实现 VLAN 间路由

如图 7-25（a）所示， Switch1 上有 VLAN1 和 VLAN2，要想实现这两个 VLAN 的路由，可以使用路由器的两个以太网接口分别接入到交换机的 VLAN1 接口和 VLAN2 接口，作为 VLAN1 和 VLAN2 的网关。



▲图 7-25 单臂路由等价图

如果路由器的以太网接口支持 802.1 Q 或 ISL，皆可以将路由器的以太网接口和交换机

的干道接口相连接，通过将路由器的物理接口分为逻辑上的接口，分别作为 VLAN1 和 VLAN2 的网关。使用这种方式实现 VLAN 间路由就是单臂路由。

路由器接口 FastEthernet 或 GigabitEthernet 支持单臂路由。

打开随书光盘中第 7 章练习“08 单臂路由.pkt”，计算机的 IP 地址已经按照图 7-25 所示配置完成，你需要在交换机上创建 VLAN 2，将 Fa0/13～24 接口指定到 VLAN 2，将交换机的 Gig1/1 配置为干道接口，配置路由器的 Gig0/0 子接口支持 VLAN1 和 VLAN2。

（1）在 Switch1 上，创建 VLAN 2，将端口指定到 VLAN 2。

```
Switch#config t
Switch (config) #vlan  2                                  --创建 VLAN 2
Switch (config-vlan) #ex
Switch (config) #interface range fastEthernet 0/13 -24
Switch (config-if-range) #switchport mode access     --指定为访问接口
Switch (config-if-range) #switchport access vlan 2  --指定到 VLAN 2
Switch (config-if-range) #exi
Switch (config) #interface gigabitEthernet 1/1
Switch (config-if) #switchport mode trunk        --将连接路由器的接口配置为干道
```

（2）在 Router0 上，配置子接口支持 VLAN。

```
Router>en
Router#config t
Router (config) #interface gigabitEthernet 0/0  --进入接口配置模式
Router (config-if) #no sh                  --物理接口需要启用，不需配置 IP 地址
Router (config-if) #ex
Router (config) #interface gigabitEthernet 0/0.1
                                          -- 0.1 子接口，使之作为 VLAN1 的网关
Router (config-subif) #encapsulation dot1Q 1
                                          --配置封装干道封装，1 代表 VLAN1 的帧标记
Router (config-subif) #ip address 192.168.1.1 255.255.255.0
                                          --为子接口添加 IP 地址
Router (config-subif) #no sh              --启用子接口
Router (config-subif) #ex
Router (config) #interface gigabitEthernet 0/0.2
                                         --0.2 子接口，使之作为 VLAN2 的网关
Router (config-subif) #encapsulation dot1Q 2
                                         --配置封装干道封装，2 代表 VLAN2 的帧标记
Router (config-subif) #ip address 192.168.2.1 255.255.255.0
                                         --为子接口添加 IP 地址
Router (config-subif) #no shutdown      --启用子接口
```

子接口的编号最好和 VLAN 的编号相同，这样好记。

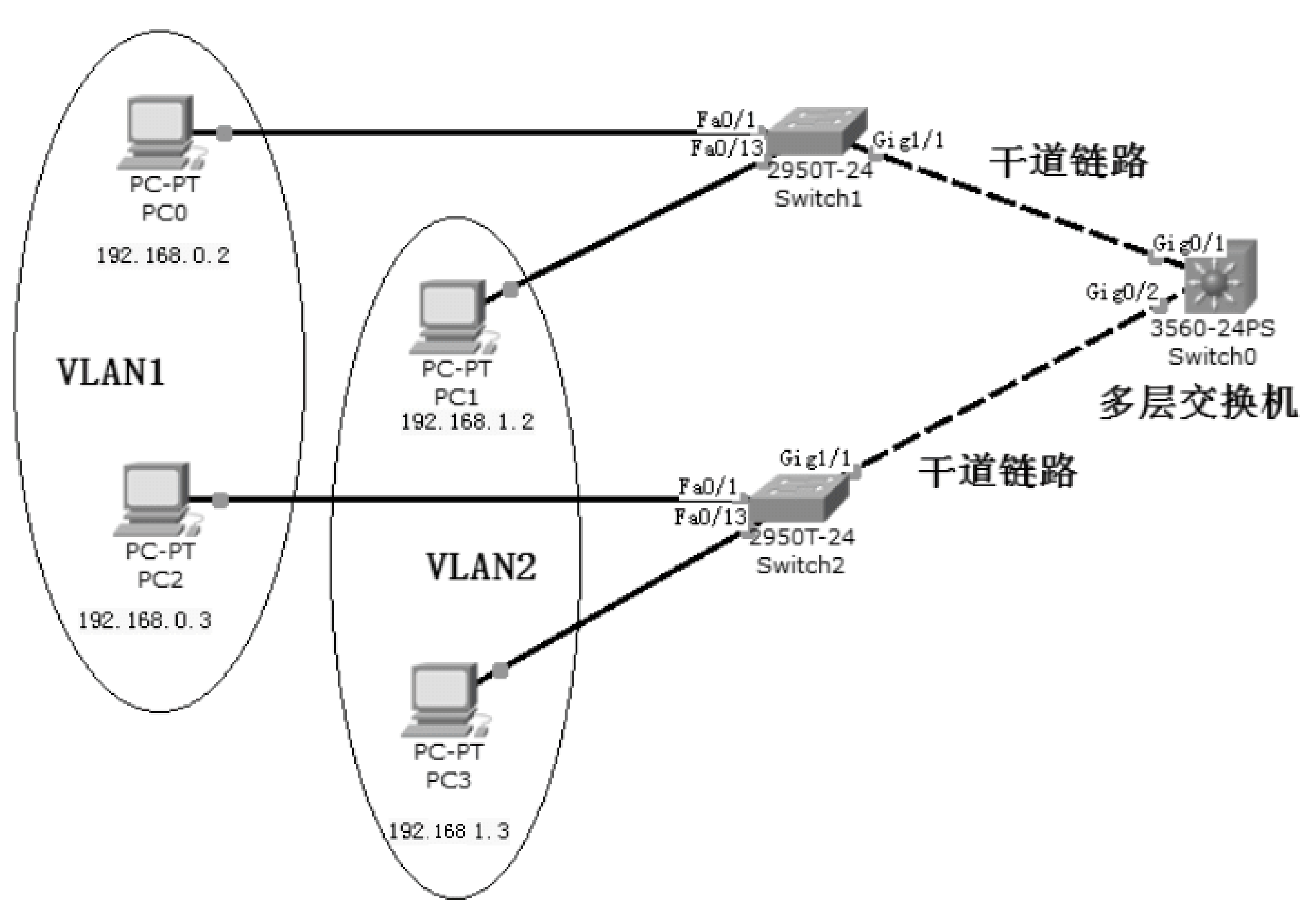
（3）PC0 ping PC1，测试 VLAN 间路由。

```
PC>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.2: bytes=32 time=40ms TTL=127
Reply from 192.168.2.2: bytes=32 time=30ms TTL=127
Reply from 192.168.2.2: bytes=32 time=24ms TTL=127
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss)
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 40ms, Average = 31ms
```

7.6.2 多层交换机实现 VLAN 间路由

使用多层交换机实现 VLAN 间路由，多层交换机虚拟接口（Switch Virtual Interface，SVI）代表一个由交换端口构成的 VLAN（其实就是通常所说的 VLAN 接口），以便于实现系统中路由和桥接的功能。一个交换机虚拟接口对应一个 VLAN，当需要路由虚拟局域网之间的流量或桥接 VLAN 之间不可路由的协议，以及提供 IP 主机到交换机连接的时候，就需要为相应的虚拟局域网配置交换机虚拟接口。其实 SVI 就是通常所说的 VLAN 接口，只不过它是虚拟的，用于连接整个 VLAN，所以将这种接口称为逻辑三层接口，也是三层接口。SVI 接口是当在 Interface VLAN 全局配置命令后面键入具体的 VLAN ID 时创建的。

打开随书光盘中第 7 章练习“08 多层交换机实现 VLAN 间路由.pkt”，网络拓扑如图 7-26 所示，网络中 VLAN1 和 VLAN2 中计算机的 IP 地址已经配置完成，网关是本网段的第一个地址。交换机之间的连接已经配置为干道链路。



▲图 7-26 多层交换机实现 VLAN 间路由

你需要配置多层交换机 Switch0 的 SVI 接口，使之支持 VLAN1 和 VLAN2 的路由，并验证 VLAN 间路由。

操作步骤如下。

（1）在 Switch0 上，配置 VLAN 接口。

```
Switch (config) #interface vlan 1  --进入 VLAN 1 的虚拟接口
Switch (config-if) #ip address 192.168.0.1 255.255.255.0
Switch (config-if) #no sh
Switch (config-if) #exi
Switch (config) #interface vlan 2
                                  --进入 VLAN 2 的虚拟接口，该命令也用于创建虚拟接口
Switch (config-if) #ip address 192.168.1.1 255.255.255.0
Switch (config-if) #no sh        --启用接口，这个命令很必要
```

（2）查看 VLAN 接口。

```
Switch#show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0010.1103.0209 (bia 0010.1103.0209)
  Internet address is 192.168.0.1/24
```

（3）在 PC0 上 ping PC3。

```
PC>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.3: bytes=32 time=33ms TTL=127
Reply from 192.168.1.3: bytes=32 time=30ms TTL=127
Reply from 192.168.1.3: bytes=32 time=12ms TTL=127
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss)
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 33ms, Average = 25ms
```

7.7 交换机 EtherChannel

EtherChannel 特性在 Switch 到 Switch、Switch 到 Router 之间提供冗余的、高速的连接方式，简单说就是将两个设备间多条 FE 或 GE 物理链路捆在一起组成一条设备间逻辑链路，从而达到增加带宽，提供冗余的目的。下面具体结合配置了解它的特点。

构成 EtherChannel 的端口必须配置成相同的特性，如双工模式、速度、同为 FE 或 GE 端口、干道状态和类型。

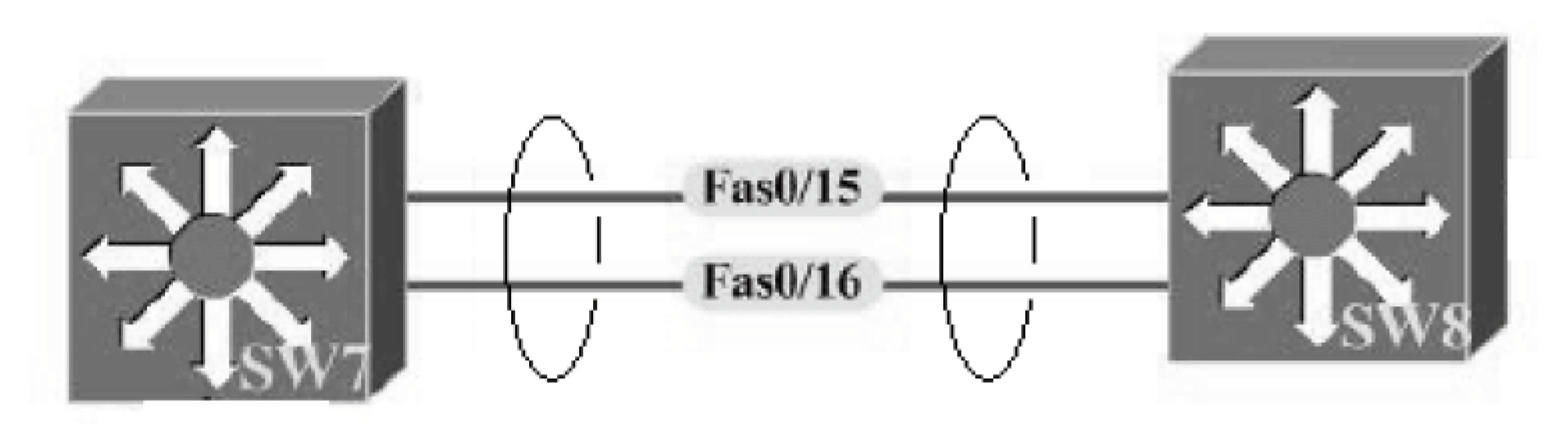
当 EtherChannel 中某一条 Link 失败时，EtherChannel 中其他链路正常工作。

当配置第二层端口作 EtherChannel 时只要在访问端口配置模式下用 channel-group n 命令指定该端口要加入的 channel-group 组，这时 Switch 会自动创建 port-channel 接口，而当配置 Layer 3 端口作 EtherChannel 时，还需要先在全局配置模式下用 interface port-channel n 命令手工创建 port-channel 接口。

Packet Tracer 不支持该实验。只能在物理交换机上进行以下实验。

1．实验环境和目标

实验环境如图 7-27 所示，SW7 和 SW8 两个交换机使用 Fa0/15 和 Fa0/16 连接，你需要将这两个链路绑定为一个 EtherChannel。



▲图 7-27　EtherChannel 示意图

2．操作步骤

（1）在 SW7 上的配置，将两个端口还原为默认配置。

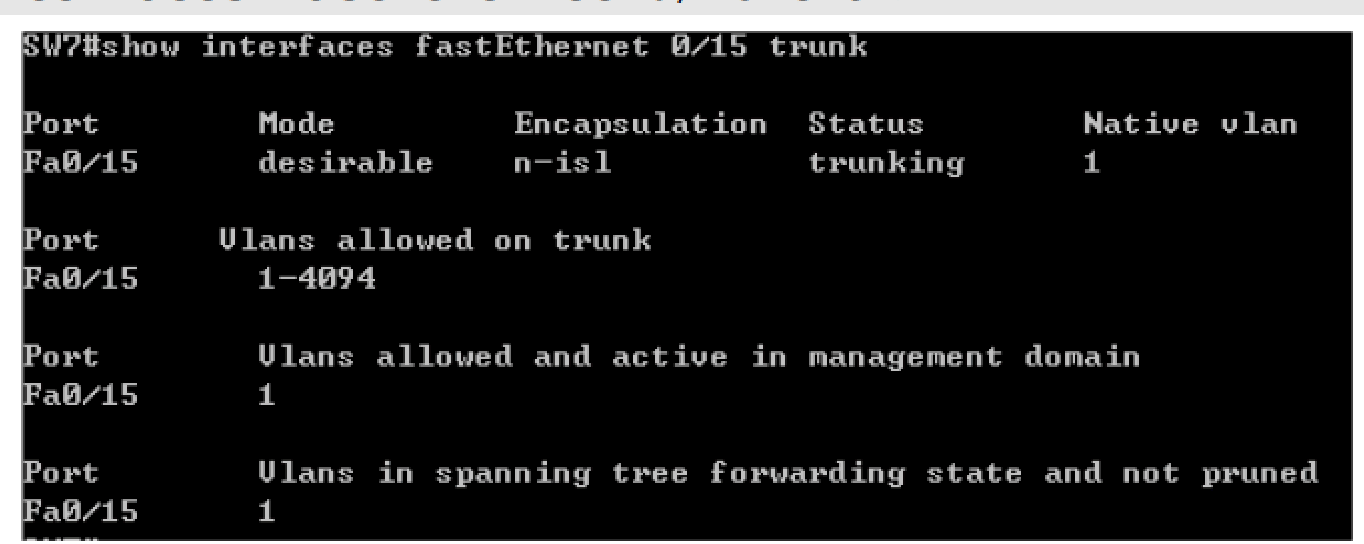
```
SW7(config)#default interface fastEthernet 0/15
SW7(config)#default interface fastEthernet 0/16
```

（2）将两个口配置为干道。

```
SW7(config)#interface range fastEthernet 0/15 - 16
SW7(config-if-range)#switchport mode dynamic desirable
```

（3）查看接口状态，Mode 为 desirable，意味着该接口期望成为干道，如图 7-28 所示。

```
SW7#show interfaces fastEthernet 0/15 trunk
```



```
SW7#show interfaces fastEthernet 0/15 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/15      desirable    n-isl          trunking      1

Port      Vlans allowed on trunk
Fa0/15      1-4094

Port        Vlans allowed and active in management domain
Fa0/15      1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/15      1
```

▲图 7-28　显示接口状态

（4）在 SW7 上，将两个接口配置成为 EtherChannel，如图 7-29 所示。

```
SW7(config)#interface range fastEthernet 0/15 - 16
SW7(config-if-range)#channel-group 1 mode desirable
```

```
SW7(config-if-range)#channel-group 1 mode desirable
SW7(config-if-range)#
04:01:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, chan
ged state to down
04:01:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, chan
ged state to down
04:01:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, chan
ged state to up
04:01:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, chan
ged state to up
04:01:47: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
04:01:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed
 state to up
            [Connection to SW7 closed by foreign host]
```

▲图 7-29　将两个接口配置为 EtherChannel

（5）以下命令查看 port-channel 1 生成树状态，可以看到是转发状态，如图 7-30 所示。

```
SW7#show spanning-tree interface port-channel 1
```

```
SW7#show spanning-tree interface port-channel 1

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------
VLAN0001            Root FWD 12        128.65   P2p Peer(STP)
```

▲图 7-30　查看配置的 channel

（6） SW7#show spanning-tree 查看生成树，Po1 接口是转发状态，该接口是 Fa0/15 和 Fa0/16 绑在一起创建的 port-channel 1 逻辑链路，如图 7-31 所示。

```
SW7#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     000a.41d7.7e80
             Cost        12
             Port        65 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000d.bd27.9400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p Peer(STP)
Po1              Root FWD 12        128.65   P2p Peer(STP)
```

▲图 7-31　在 SW7 上查看生成树端口

（7）在 SW8 上进行相同的配置，查看生成树，如图 7-32 所示。

```
SW8#show spanning-tree

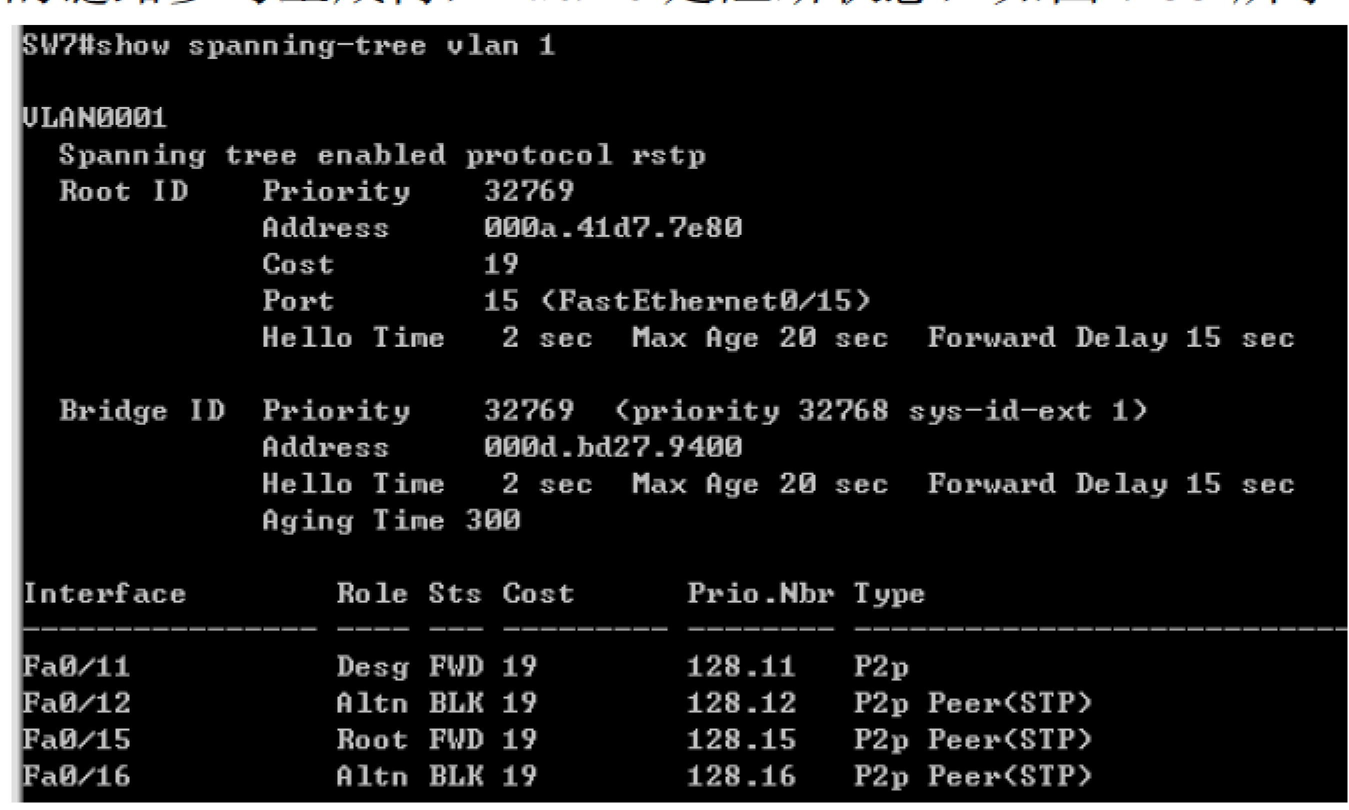
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.41d7.7e80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000a.41d7.7e80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/13           Desg FWD 19        128.13   P2p
Po1              Desg FWD 12        128.65   P2p
```

▲图 7-32　在 SW8 上查看生成树

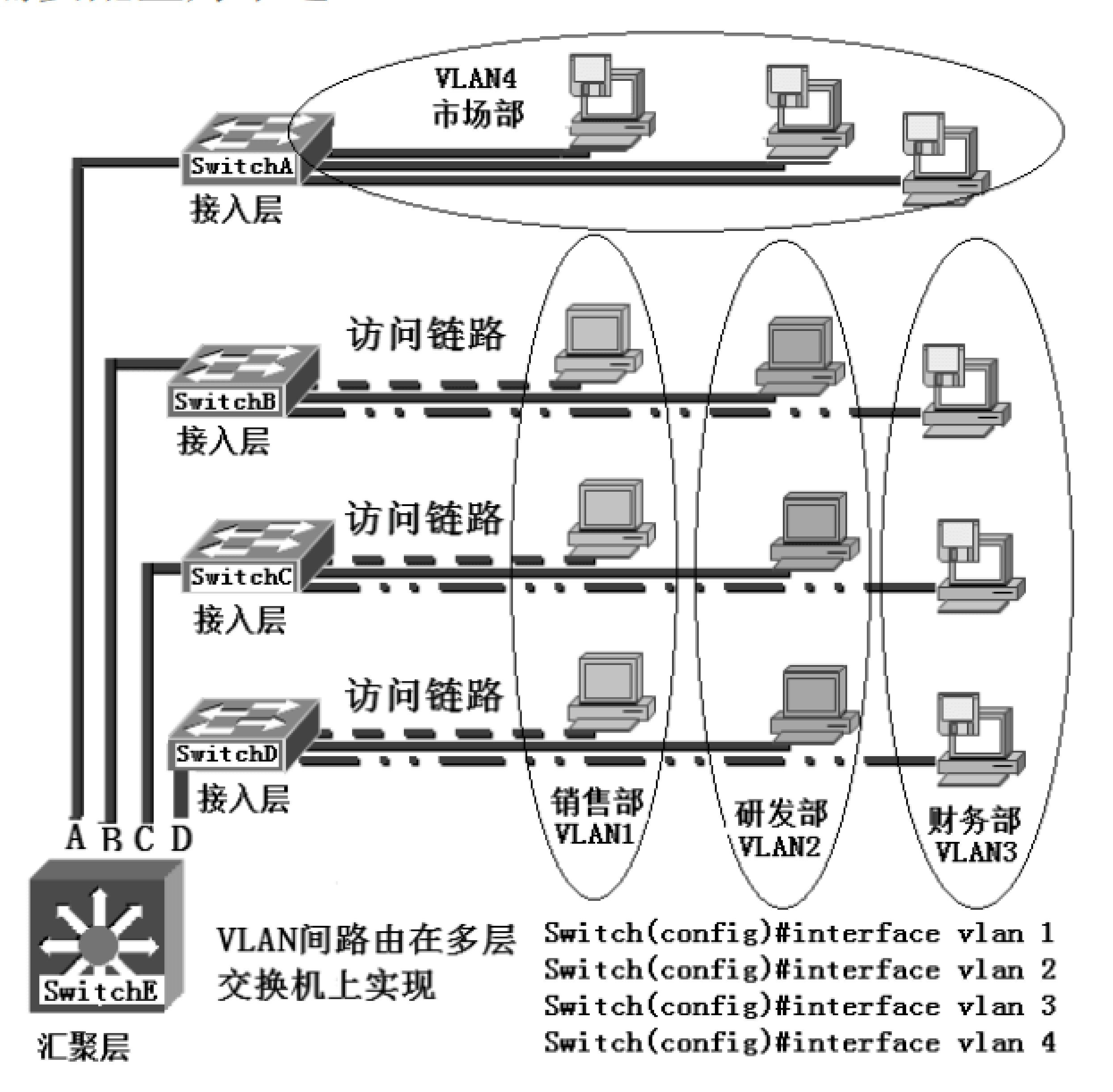
（8）把端口设置为默认之后，再查看 VLAN 1 的生成树端口，可以看到 Fa0/15 和 Fa0/16 作为单独的链路参与生成树，Fa0/16 是阻断状态，如图 7-33 所示。



▲图 7-33 查看端口状态

7.8 习 题

1. 网络如图 7-34 所示，在汇聚层交换机实现 VLAN 间路由，请问与汇聚层交换机连接的哪些链路需要配置为干道？



▲图 7-34 需要配置为干道的链路

2. 以太网交换机工作在 OSI 的＿（1）＿，并按照＿（2）＿来进行信息转发的决策。以太网交换机上的每个端口都可以绑定一个或多个＿（3）＿。

（1）A. 物理层　　B. 数据链路层
C. 网络层　　D. 传输层

（2）A. 端口的 IP 地址　　B. 数据包中的 MAC 地址

C. 网络广播　　　　D. 组播地址

（3）A. 网关地址　　　　B. LLC 地址

C. MAC 地址　　　　D. IP 地址

3. 组建局域网可以用集线器，也可以用交换机。用集线器连接的一组工作站__（1）__，用交换机连接的一组工作站__（2）__。

（1）A. 同属于一个冲突域，但不属于一个广播域

B. 同属于一个冲突域，也同属于一个广播域

C. 不属于一个冲突域，但同属于一个广播域

D. 不属于一个冲突域，也不属于一个广播域

（2）A. 同属于一个冲突域，但不属于一个广播域

B. 同属于一个冲突域，也同属于一个广播域

C. 不属于一个冲突域，但同属于一个广播域

D. 不属于一个冲突域，也不属于一个广播域

4. 一个园区网内某 VLAN 中的网关地址设置为 195.26.16.1，子网掩码设置为 255.255.240.0，则 IP 地址__（1）__不属于该 VLAN。该 VLAN 最多可以配置__（2）__台 IP 地址主机。

（1） A. 195.26.15.3　　　　B. 195.26.18.128

C. 195.26.24.254　　　　D. 195.26.31.64

（2） A. 1021　　　　B. 1024

C. 4093　　　　D. 4096

5. VLAN 中，每个虚拟局域网组成一个__（1）__，如果一个 VLAN 跨越多个交换机，则属于同一 VLAN 的工作站要通过__（2）__互相通信。

（1）A. 区域　　　　B. 组播域

C. 冲突域　　　　D. 广播域

（2）A. 应用服务器　　　　B. 主干（Trunk）线路

C. 环网　　　　D. 本地交换机

6. 在默认配置的情况下，交换机的所有端口__（1）__。连接在不同交换机上的、属于同一 VLAN 的数据帧必须通过__（2）__传输。

（1）A. 处于直通状态　　　　B. 属于同一 VLAN

C. 属于不同 VLAN　　　　D. 地址都相同

（2）A. 服务器　　　　B. 路由器

C. Backbone 链路　　　　D. Trunk 链路

7. 虚拟局域网中继协议（VTP）有三种工作模式，即服务器模式、客户机模式和透明模式，以下关于这三种工作模式的叙述中，不正确的是______。

A. 在服务器模式下可以设置 VLAN 信息

B. 在服务器模式下可以广播 VLAN 信息

C. 在客户机模式下不可以设置 VLAN 信息

D. 在透明模式下不可以设置 VLAN 信息

8. 在下面关于 VLAN 的描述中，不正确的是________。

A. VLAN 把交换机划分成多个逻辑上独立的交换机

B. 主干链路（Trunk）可以提供多个 VLAN 之间通信的公共通道

C. 由于包含了多个交换机，所以 VLAN 扩大了冲突域

D. 一个 VLAN 可以跨越交换机

9. 下面有关 VLAN 的语句中，正确的是______。

A. 虚拟局域网中继协议 VTP（VLAN Trunk Protocol ）用于在路由器之间交换不同 VLAN 的信息

B. 为了抑制广播风暴，不同的 VLAN 之间必须用网桥分隔

C. 交换机工作在 VTP 服务器模式，这样可以把 VLAN 的配置信息通告给其他交换机

D. 一台计算机可以属于多个 VLAN，即它可以访问多个 VLAN，也可以被多个 VLAN 访问

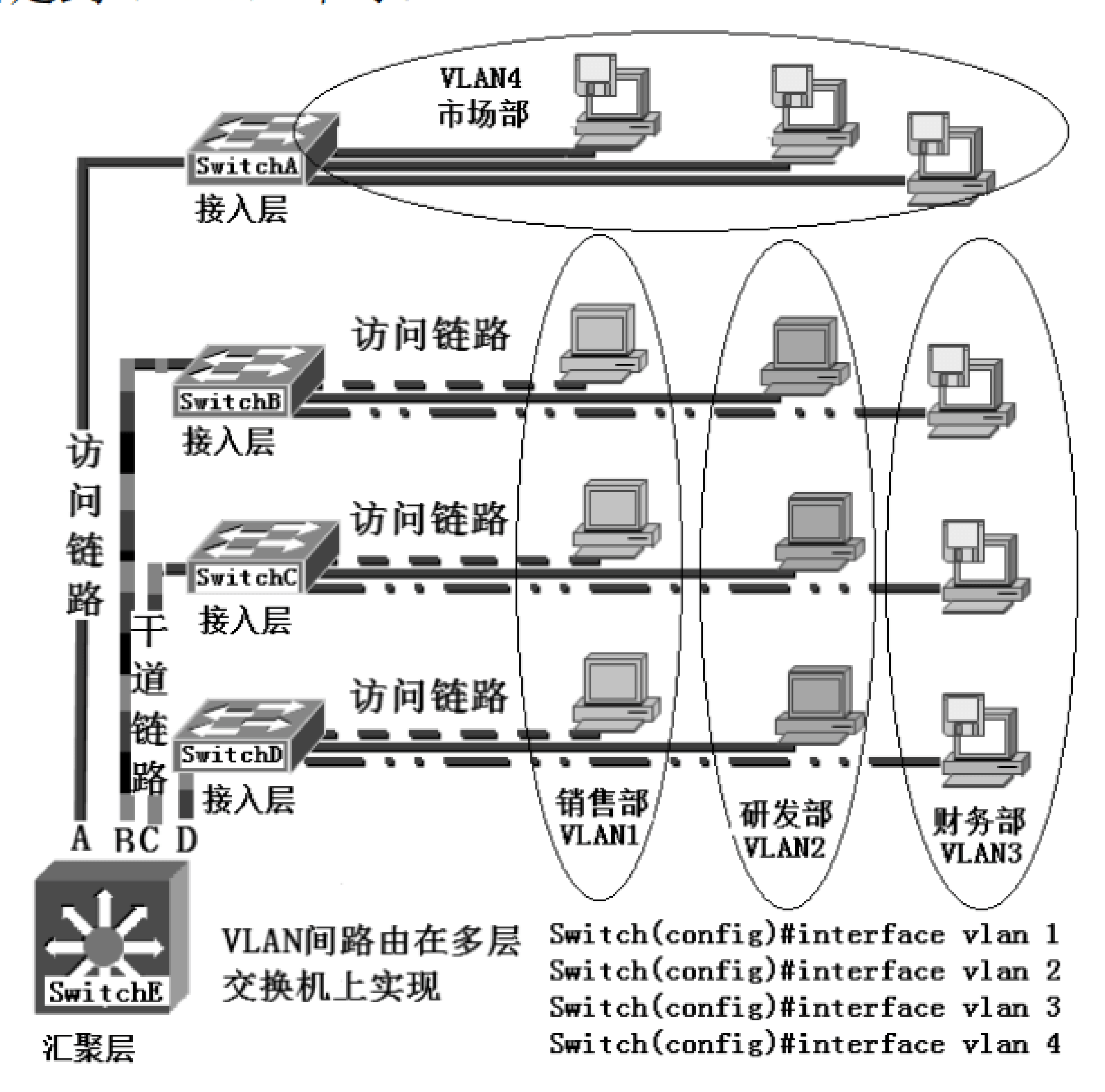
10. 划分 VLAN 的方法有多种，这些方法中不包括______。

A. 根据端口划分　　B. 根据路由设备划分

C. 根据 MAC 地址划分　　D. 根据 IP 地址划分

习题答案

1. 配置为干道链路的有 B、C、D。由于在 SwitchA 上只有一个 VLAN，因此 A 链路可以配置为访问链路，在汇聚层交换机上需要将 A 接口配置为 Access 接口，并将其指定到 VLAN4 即可。



2. （1）B （2）B （3）C
3. （1）B （2）C
4. （1）A （2）C 因为路由器已经用了一个 IP 地址，可用的主机地址还剩下 16×256－3=4093
5. （1）D （2）B
6. （1）B （2）D
7. D
8. C
9. C
10. B 、D

第 8 章　网 络 安 全

作为一个系统管理员，保护敏感重要的数据和网络资源、防止可能的恶意入侵，是最优先考虑的事情。网络安全的范畴很广泛，包括物理层安全、数据链路层安全、网络层安全、传输层安全以及应用层安全，但是本章的重点在于网络层安全。

通过在路由器上配置访问控制列表，可以实现数据流量过滤，从而实现网络层安全。比如不允许财务部门计算机所在的网段访问 Internet，销售部的计算机所在的网段能够访问 Internet 上网站但不允许上网聊天，禁止 Internet 的黑客使用地址欺骗攻击内网。

本章主要内容：

- 从 OSI 参考模型来看网络安全
- 典型的安全网络架构
- 安全威胁
- 标准访问控制列表
- 扩展访问控制列表
- 使用访问控制列表保护路由安全
- 基于时间的访问控制列表
- 使用 ACL 降低安全威胁

8.1 网络安全简介

在讲解路由器上实现网络层安全之前，先从广义上为大家介绍一下网络安全涉及的范围。

8.1.1 从 OSI 参考模型来看网络安全

在工作中可能会听到这样的词“物理层安全”、“数据链路层安全”、“网络层安全”、“应用层安全”，这些都是根据 OSI 参考模型的分层来说的。

OSI 参考模型将数据通信分为 7 层：应用层、表示层、会话层、传输层、网络层、数据链路层和物理层。网络安全也可以从这个角度来分类。

下面针对 OSI 参考模型的层列举一些安全的例子。

1. 物理层安全

通过网络设备进行攻击：Hub 和无线 AP 进行攻击。攻击者将计算机连接到使用 Hub 组建的网络中就可以捕获其他用户通信的数据包。无线 AP 如果没有安全措施，攻击者可以捕获无线 AP 通信。再比如，你公司的办公大楼，其中一层租给保险公司，这一层的办公室的网线还在你公司的交换机上连接，并且没有禁用这些端口，保险公司就可以将计算机轻易接入到你公司的网络，这就是物理层不安全。

物理层安全措施：使用交换机替代 Hub，为无线 AP 配置密码实现无线设备的接入保护和实现数据加密通信。

2. 数据链路层安全

数据链路层攻击：恶意获取数据或 MAC 地址。由于大多数 IDS 和操作系统对网络层以下的防御很弱，因此很危险。攻击方式有 ARP 欺骗、ARP 广播，同一网段有重复的 MAC 地址。

数据链路层安全措施：在交换机的端口上控制连接计算机的数量或绑定 MAC 地址，这些都是数据链路层安全。在交换机上划分 VLAN 也属于数据链路层安全。在计算机和路由器上添加 IP 地址和 MAC 地址绑定可防止 ARP 欺骗。ADSL 拨号上网的账号和密码实现的是数据链路层安全。

3. 网络层安全

网络层攻击：IP Spoofing（IP 欺骗）、Fragmentation Attacks（碎片攻击）、Reassembly attacks（重组攻击）、Ping of death（Ping 死攻击）。

网络层安全措施：在路由器上设置访问控制列表和 IPSec、在 Windows 上实现的 Windows 防火墙和 IPSec，这些都属于网络层安全。

4. 传输层安全

传输层攻击：Port Scan（端口扫描）、TCP reset attack（TCP 重置攻击）、SYN DoS floods（SYN 拒绝服务攻击）、LAND attack（LAND 攻击）、Session hijacking（会话劫持）。

5. 应用层安全

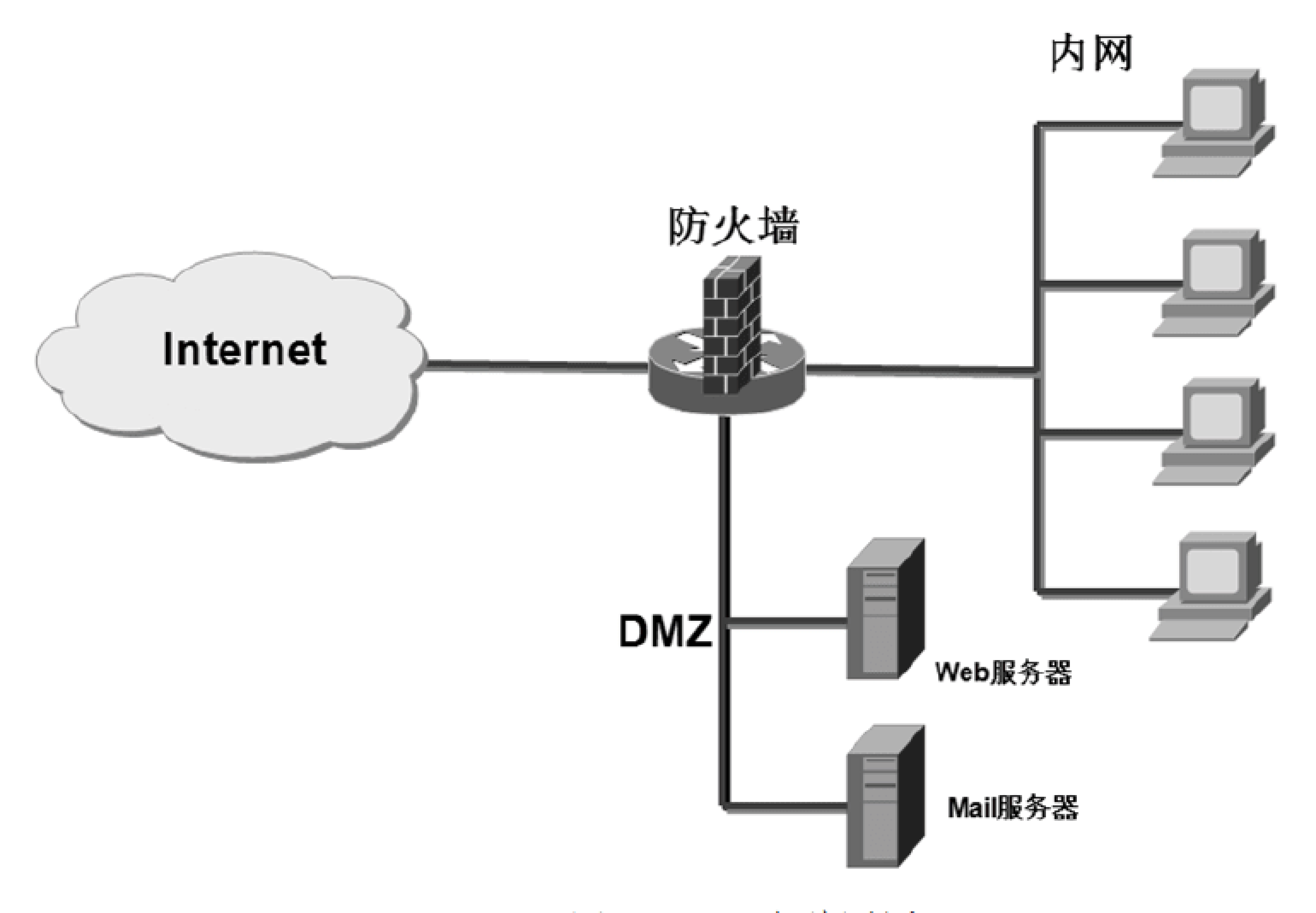
应用层攻击：MS-SQL Slammer worm 缓冲区溢出、IIS 红色警报、E-mail 蠕虫、蠕虫、病毒、木马、垃圾邮件、IE 漏洞。

安全措施：安装杀毒软件，更新操作系统。

8.1.2 典型的安全网络架构

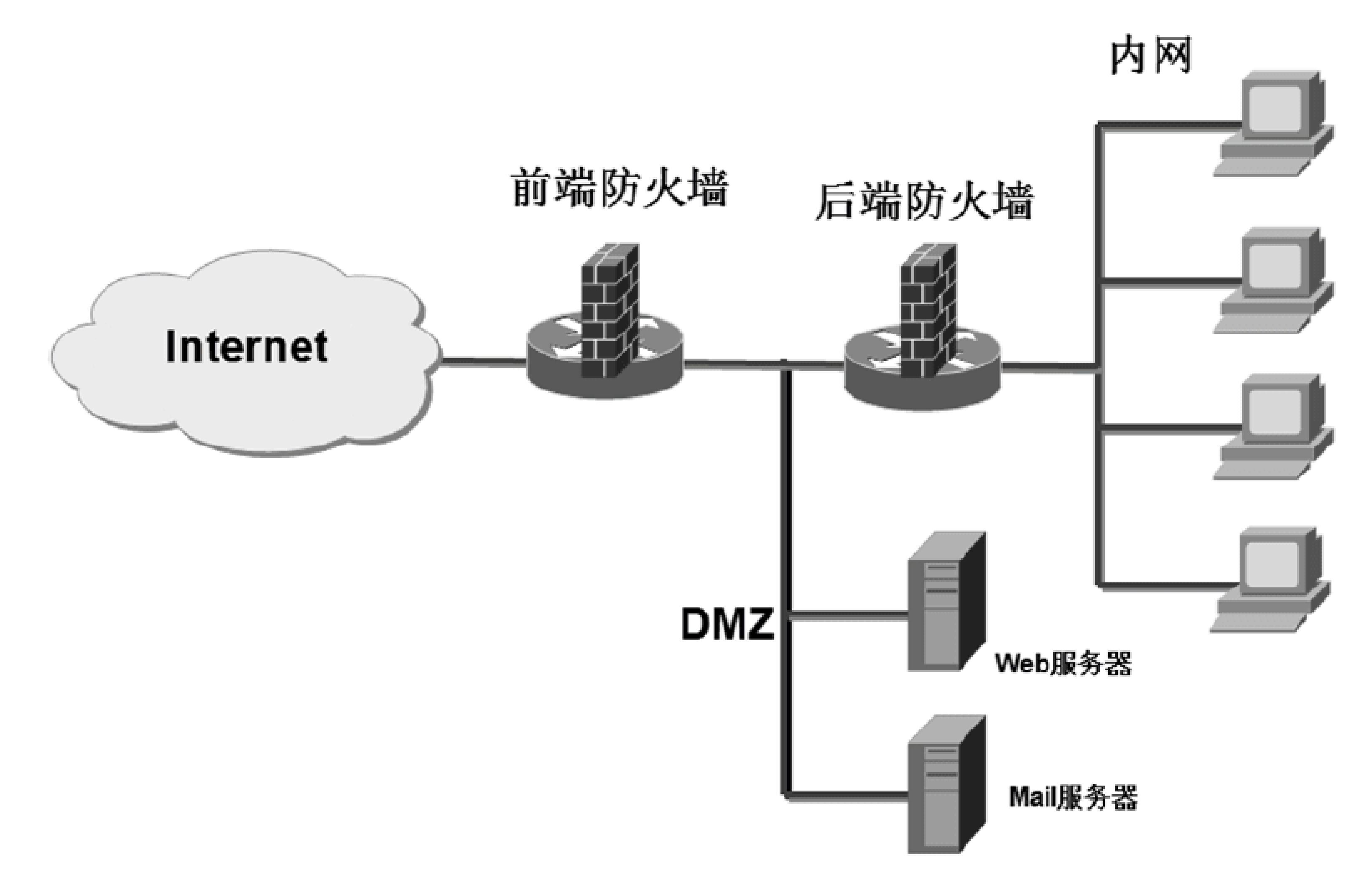
许多大中型企业网络中，各种各样的安全策略都是基于内网、非军事区（DMZ）路由器以及防火墙设备的。防火墙通过屏蔽各部分的网络流量来提供附加的安全保障，而进行这些工作需要使用访问控制列表。

典型的网络架构如图 8-1 所示的三向外围网，防火墙设备连接 Internet、内网和 DMZ 区。DMZ 区部署了公司对外的 Web 和 Mail 服务器，一般是公网 IP 地址。内网是私网 IP 地址，一般不对 Internet 用户提供服务，但是需要访问 Internet。如果入侵者突破了该防火墙，就威胁到 DMZ 和内网的安全。



▲图 8-1　三向外围网

另外一种典型的网络架构就是背靠背防火墙，如图 8-2 所示，两个防火墙之间是 DMZ 区，内网在防火墙后端。建议这两个防火墙不是同一家公司的产品，比如前端使用 Cisco 公司的 PIX 防火墙，后端使用微软的软件防火墙 ISA 2006。这样入侵者要想入侵内网，就需要突破两个不同厂商的防火墙，增加了难度。



▲图 8-2　背靠背防火墙

8.1.3　防火墙的种类

防火墙总体上分为包过滤、应用级网关和代理服务等几大类型。

1. 数据包过滤

数据包过滤（Packet Filtering）技术是在网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，被称为访问控制列表（Access Control List，ACL）。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合来确定是否允许该数据包通过。数据包过滤防火墙逻辑简单、价格便宜、易于安装和使用，网络性能和透明性好，它通常安装在路由器上。路由器是内部网络与 Internet 连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

数据包过滤又称为网络级别防火墙，网络级别的防火墙很快，在今天你仍然可以在许多网络设施上找到它们的身影，特别是在路由器上。但是不能基于数据包的内容过滤数据。

2. 应用级网关

应用级网关（Application Level Gateways）是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告。实际中的应用网关通常安装在专用工作站系统上。

数据包过滤和应用网关防火墙有一个共同的特点，就是它们仅仅依靠特定的逻辑判定是否允许数据包通过。一旦满足逻辑，防火墙内外的计算机系统则建立直接联系，防火墙外部的用户便有可能直接了解防火墙内部的网络结构和运行状态，这有利于实施非法访问和攻击。

3. 代理服务

代理服务（Proxy Service）也称链路级网关或 TCP 通道（Circuit Level Gateways or TCP Tunnels），也有人将它归于应用级网关一类。它是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”由两个终止代理服务器上的“链接”来实现，外部计算机的网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。此外，代理服务也对过往的数据包进行分析、注册登记，形成报告，同时当发现被攻击迹象时会向网络管理员发出警报，并保留攻击痕迹。国内代理服务器软件有 CCProxy，微软的代理服务器软件 ISA2006。

防火墙能有效地防止外来入侵，它在网络系统中的作用如下。

- 控制进出网络的信息流向和信息包。
- 提供流量统计和审计。
- 隐藏内部 IP 地址及网络结构的细节。
- 入侵检测且对检测到的入侵采取响应。

8.1.4 常见的安全威胁

因特网变成今天如此重要的工具，是它的创建者绝对想不到的。在网络设计阶段就没有很好地将安全考虑进去，这也是为什么安全会变成如此大的问题的原因——TCP/IP 与生俱来就是不安全的。Cisco 有许多窍门帮助我们来处理这些问题，下面让我们来分析一些常见的攻击。

1. 应用层攻击

这些攻击通常瞄准运行在服务器上的软件漏洞，而这些漏洞众所周知。比如，服务器运行 FTP、Mail、HTTP 服务都有可能有漏洞。因为这些账户的许可层都获得了一定的特权，如果这台计算机正在运行以上提到的应用程序中的一种，恶意者就可以访问并掠取计算机资源。

2. Autorooters

你可以把它想象为一种黑客机器人。恶意者使用某种叫做 Rootkit 的东西来探测、扫描并从目标计算机上捕获数据，装了 Rootkit 后的目标计算机像是在整个系统中装了“眼睛”一样，自动监视着整个系统。

3. 后门程序

后门程序是通往一个计算机或网络的简洁路径。经过简单入侵或是经过更精心设计的特洛伊木马代码，恶意者可使用植入攻击进入一台指定的主机或是网络，无论何时它们都可进入——除非你发觉并阻止它们。

4. 拒绝服务（DoS）和分布式拒绝服务器（DDoS）攻击

这些攻击很恶劣——摆脱它们同样也很费力。即使黑客们都鄙视使用这种攻击的黑客（因为它们如此令人厌恶），但是它们真的很容易就能实现。从根本上说，当一个服务超范围索取系统正常提供它的资源时，它将变得不正常，而且存在不同的攻击风格。

- TCP SYN 泛洪攻击：发生在一个客户端发起表面上普通的 TCP 连接并且发送 SYN 信息到一台服务器时。这台服务器通过发送 SYN-ACK 信息到客户端进行响应，这样就通过往返 ACK 信息建立连接。听起来很好，但正是在这个过程（当连接仅有一半打开的时候）中，受害的计算机将完全被蜂拥而至的半打开连接所淹没，最终导致瘫痪。
- “死亡之 ping”攻击：你可能知道 TCP/IP 的最大包大小为 65536 字节。不知道也没关系，仅需要了解这种攻击通过使用大量数据包进行 ping 操作来实行攻击，这些数据包可导致设备不间断地重启、停滞或完全崩溃。

5. IP 欺骗

这有点像它的名字，恶意者从你的网络内部或外部，通过做下列两件事之一：以你的内部网络可信地址范围中的 IP 地址呈现或者使用一个核准的、可信的外部 IP 地址，来伪装成一台可信的主机。因为黑客的真实身份被隐藏在欺骗地址之下，所以这常常仅是你的难题的开始。

6. 中间人攻击

是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”，然后入侵者把这台计算机模拟一台或两台原始计算机，使“中间人”能够与原始计算机建立活动连接并允许其读取或修改传递的信息，但是两个原始计算机用户却认为它们是在互相通信。

7. 网络侦察

在入侵一个网络之前，黑客经常会收集所有关于这个网络的信息，因为他们对这个网络知道得越多，越容易对它造成危害。他们通过类似端口扫描、DNS 查询、ping 扫描等方法实现他们的目的。

8. 包嗅探

包嗅探的工作原理：网络适配卡开始工作于混杂模式，它发送的所有包都可以被一个特殊的应用程序从网络的物理层窃取，并进行查看及分类。包嗅探常窃取一些价值高、敏感的数据，其中包括口令和用户名，在实施身份盗取时能获得超值信息。

9. 口令攻击

口令攻击有许多方式，可经由多种较成熟类型的攻击实现。这些攻击包括 IP 欺骗、包嗅探以及特洛伊木马，它们唯一的目的就是发现用户的口令，这样，它们就可以伪装成一个合法的用户，访问用户的特许操作及资源。

10. 强暴攻击

强暴攻击是另一种面向软件的攻击，使用运行在目标网络的程序尝试连接到某些类型的共享网络资源。如果访问账户拥有很多特权，对于黑客来说这是非常完美的，因为这些恶意者可以开启后门，再次访问就可以完全绕过口令。

11. 端口重定向攻击

端口重定向攻击要求黑客已经侵入主机，并经由防火墙得到被改变的流量（这些流量通常是不被允许通过的）。

12. 特洛伊木马攻击和病毒

这两种攻击实际上比较相似：特洛伊木马和病毒都使用恶意代码感染用户计算机，使得用户计算机遭受不同程度的瘫痪、破坏甚至崩溃。但是它们之间还是有区别的：病毒是真正恶意程序，附着在 command.com 文件之上，而 command.com 又是 Windows 系统的主要解释文件。病毒接着会疯狂地运行，删除文件并且感染计算机上任何 command.com 的文件；特洛伊木马是一个封装了秘密代码的真正的完整应用程序，这些秘密代码使得它们呈现为完全不同的实体，表面上像是一个简单、天真的游戏，实际上具有丑陋的破坏工具的本质。

13. 信任利用攻击

信任利用攻击发生在内网之中，由某些人利用内网中的可信关系来实施。例如，一个公司的非军事网络连接中通常运行着类似 SMTP、DNS 以及 HTTP 服务器等重要的东西，一旦和它们处在同一网段时，这些服务器很容易遭受攻击。

在这里不打算详细介绍如何降低上述每一种安全威胁，不仅是因为这将超出本书的范围，也是因为我打算教给你的将是真正保护你远离攻击的一般方法。

因此，基本上可以认为本章在讲述如何实现“网络层安全”。

8.2 访问控制列表

你公司可能有多个部门，每个部门的计算机有一个单独的 VLAN，公司的路由器实现 VLAN 间路由且连接 Internet。如果你打算只允许市场部门的计算机也就是 VLAN1 能够访问 Internet 的资源，而不允许 QQ、MSN 等聊天工具登录；销售部门的计算机不允许访问 Internet，如何实现这样的控制呢？

路由器不但能够在不同网段转发数据包，而且还能够基于数据包的目标地址、源地址、协议和端口号来允许特定的数据包通过或拒绝通过。要实现这样的控制需要在路由器定义访问控制列表（ACL），并将这些 ACL 绑定到路由器的接口。

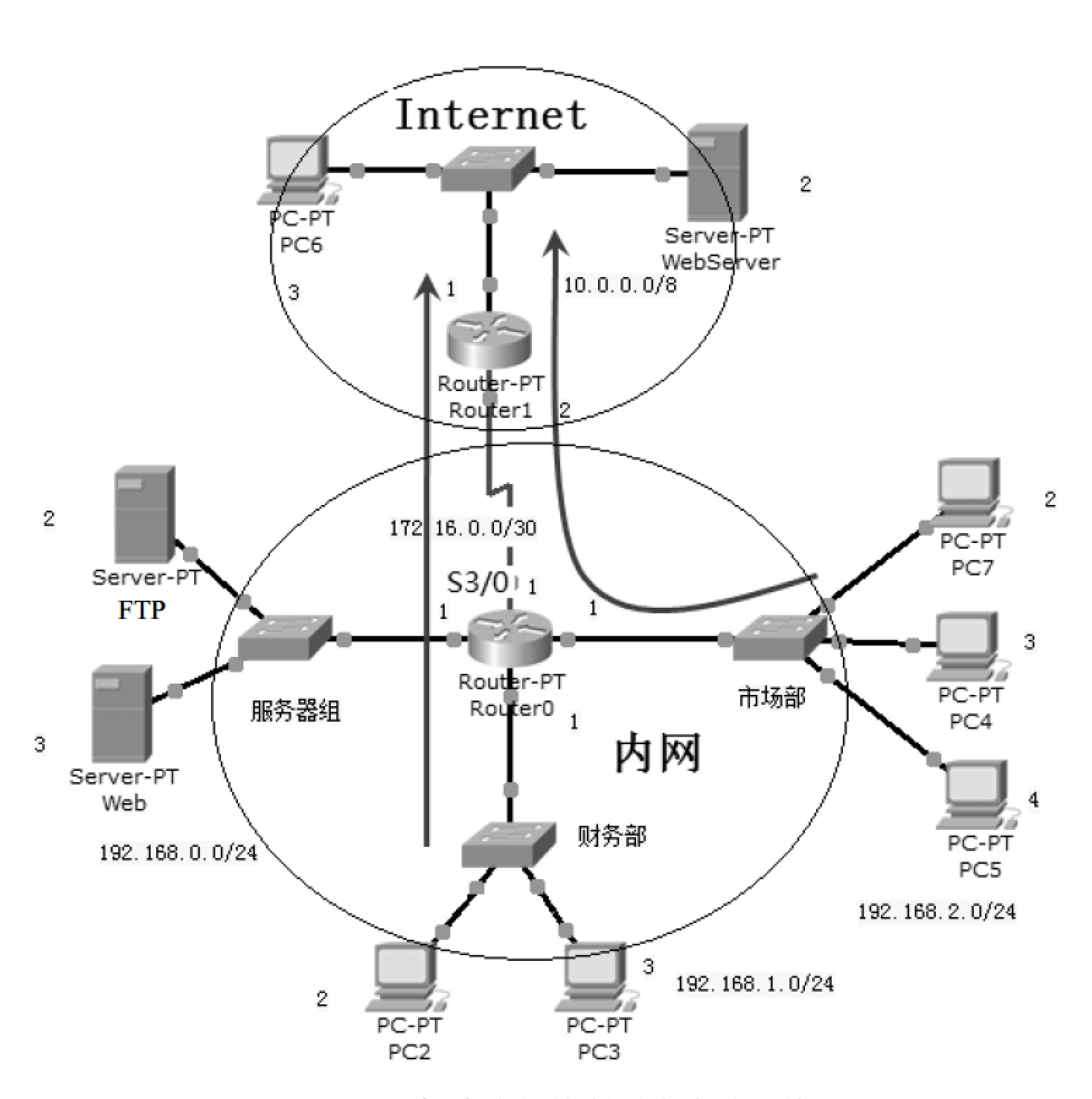
下面将会为大家介绍两种类型的访问控制列表，即标准访问控制列表和扩展访问控制列表。

8.2.1 标准访问控制列表

标准访问控制列表只基于 IP 数据包的源 IP 地址作为转发或是拒绝的条件。所有决定是基于源 IP 地址的，这意味着标准的访问控制列表基本上允许或拒绝整个协议组。它们不区分 IP 流量类型，例如 Telnet、UDP 等服务。

打开随书光盘中第 8 章练习“01 标准访问控制列表.pkt”，网络拓扑如图 8-3 所示，网络中的路由器和计算机的 IP 地址已经按照拓扑中的标识地址配置完成，路由器上配置了相应的路由。Router0 是企业内网的路由器，内网有三个网段；Router1 模拟的是 Internet 上的路由器。

要求	只允许市场部和财务部的计算机访而服务器组的计算机拒绝访问 Internet。



▲图 8-3 标准访问控制列表实验环境

在路由器 Router0 上定义访问控制列表，将其作为 Router0 的 S3/0 接口的出站访问控制列表，因为市场部和财务部的计算机要访问 Internet 必须从 Router0 的 S3/0 接口转发出去。

操作步骤如下。

（1）使用 PC7 ping WebServer、FTP ping WebServer，发现都能通。如果没有配置 ACL，默认网络是畅通的。

```
PC>ping 10.0.0.2
```

（2）在 Router0 上创建 ACL。

```
Router>en
Router#config t
Router（config）#access-list ?
  <1-99>     IP standard access list     --标准 ACL 的编号范围是 1～99
  <100-199>  IP extended access list     --扩展 ACL 的编号范围是 100～199
Router（config）#access-list 10 permit 192.168.2.0 0.0.0.255
Router（config）#access-list 10 permit 192.168.1.0 0.0.0.255
```

提示

以上命令定义了一个标准访问控制列表 10，标准访问控制列表的编号可以是 1～99 之间的任何值。
后面的 0.0.0.255 是反转掩码，也就是二进制的子网掩码中将 0 变成 1、1 变成 0，然后写成十进制。
该 ACL 10 允许源地址是 192.168.2.0 255.255.255.0 和 192.168.1.0255.255.255.0 网段的数据包通过。
访问控制列表的 any 和 0.0.0.0 255.255.255.255 等价。

（3）将 ACL 10 绑定到 Router0 的 S3/0 出口。

```
Router（config）#interface Serial 3/0
Router（config-if）#ip access-group 10 ?
  in   inbound packets                          --in 表示进入接口时检查
  out  outbound packets                         --out 表示出接口时检查
Router（config-if）#ip access-group 10 out      --标准 ACL 10 出去时检查
使用 PC7 ping WebServer，发现能够 ping 通
使用 FTP ping WebServer，有以下输出:
Reply from 192.168.0.1: DestiNATion host unreachable.
```

ACL 拦截后，返回计算机目标主机不可到达的。可以看到 ACL 默认隐含拒绝所有流量。

总结

每个接口、每个协议或每个方向只能分派一个访问列表，这意味着如果创建了 IP 访问列表，每个接口只可以有一个入口访问列表和一个出口访问列表。
除非在访问列表末尾有 permit any 命令，否则所有和列表测试条件不符的数据包都将被丢弃。
每个列表应该至少有一个允许语句，否则将会拒绝所有流量。
先创建访问列表，然后将列表应用到一个接口。任何应用到接口的访问列表如果不是现成的访问列表，那么此列表不会过滤流量。
访问列表设计为过滤通过路由器的流量，但不过滤路由器产生的流量。

修改现有的访问控制列表

继续以上的实验。

上面的实验已经在 Router0 上配置了标准的访问控制列表 10，只允许市场部和财务部的计算机能够访问 Internet，但是拒绝市场部计算机 PC7 访问 Internet。如何更改访问控制列表才能达到以上目的。

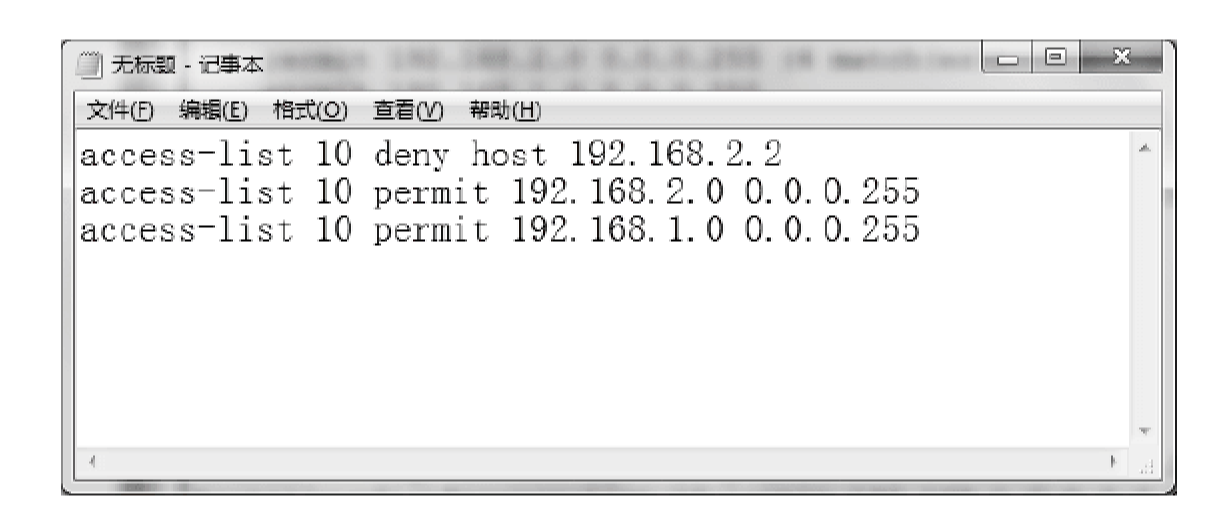
在 ACL 10 中添加一条拒绝主机 192.168.2.2 的设置。

```
Router（config）#access-list 10 deny host 192.168.2.2
host 192.168.2.2 等价于 192.168.2.2 0.0.0.0。
```

使用 PC7 ping WebServer 发现还是能够通。设置不起作用，为什么呢？

```
Router（config）#^Z
Router#show access-lists 10                              --查看 ACL
Standard IP access list 10
   permit 192.168.2.0 0.0.0.255 （4 match（es）          --第 1 条
   permit 192.168.1.0 0.0.0.255                          --第 2 条
   deny host 192.168.2.2                                 --第 3 条
```

> **提示**
>
> 我们看到 ACL 中的顺序和添加时的顺序一致。
>
> 路由器在应用访问控制列表时，会逐一从上到下检查，如果发现匹配的就不再检查 ACL 中后面的设置。拒绝主机 192.168.2.2 的第 3 条不会用上，因为第 1 条就已经允许了。
>
> 因此需要将第 3 条的设置放置到第 1 条的位置，但是路由器没有为你提供调整顺序的功能，需要删除 ACL，重新创建。这里有一个技巧，你可以在记事本中将 ACL 的顺序调整好，如图 8-4 所示，再将记事本中的内容直接粘贴到全局配置模式下路由器配置的 CLI。



▲图 8-4 记事本中的内容

```
Router（config）#no access-list 10    --删除 ACL 10 的所有设置
Router（config）#access-list 10 deny host 192.168.2.2
Router（config）#access-list 10 permit 192.168.2.0 0.0.0.255
Router（config）#access-list 10 permit 192.168.1.0 0.0.0.255
```

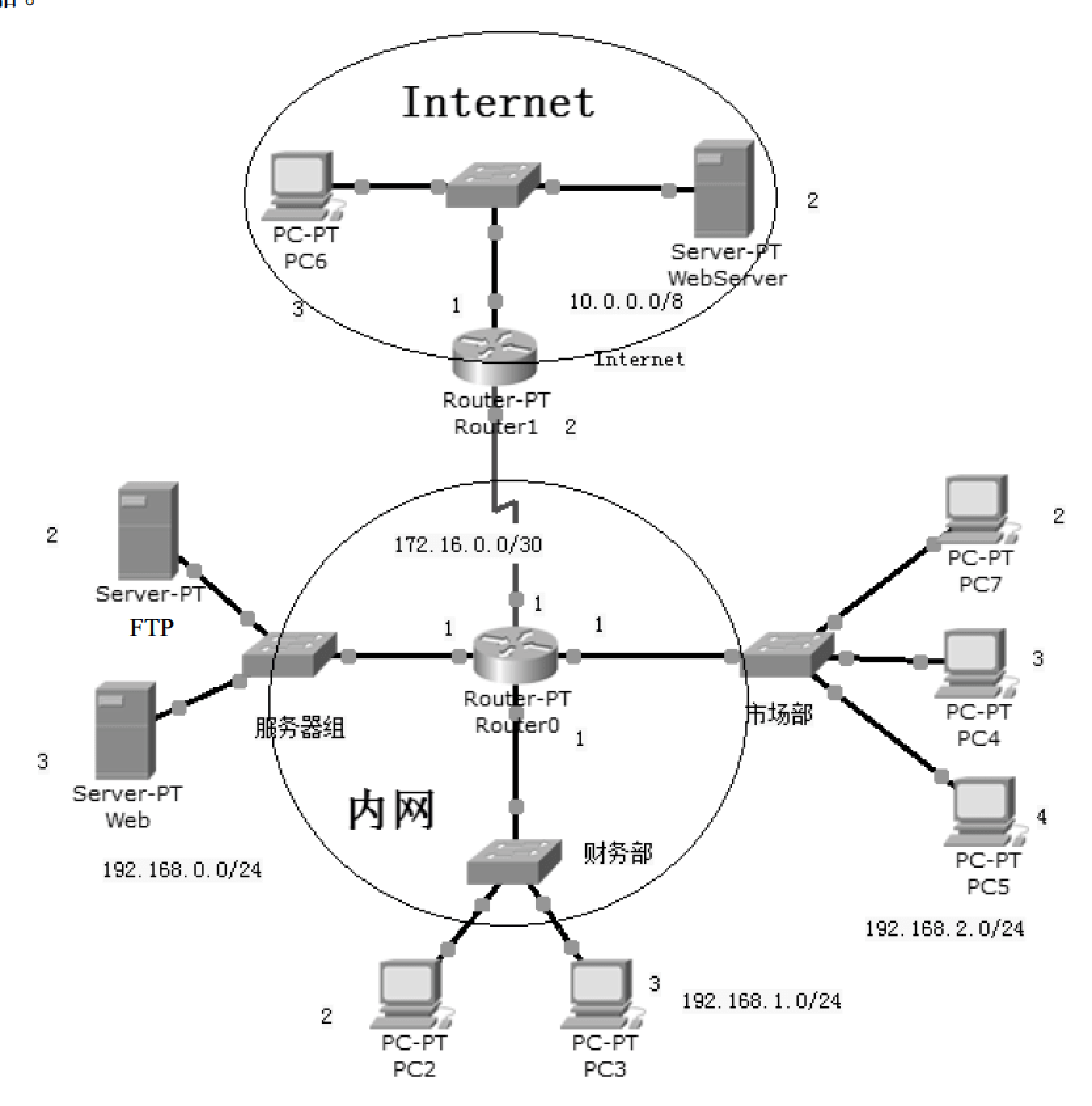
用 PC7 ping WebServer 不能通，使用 PC4 ping WebServer 能够通，达到了预期的目的。

总结	组织好访问控制列表，要将更加具体的地址或网段放在访问控制列表的最前面。任何时候访问列表添加新条目时，将把新条目放置到列表的末尾。强烈推荐使用文本编辑器编辑访问列表。 不能从访问列表中删除一行。如果试着这样做，将删除整个列表。最好在编辑列表之前将访问列表复制到一个文本编辑器中。只有使用命名访问列表时例外。

8.2.2 扩展访问控制列表

扩展访问控制列表可以基于 IP 包的第 3 层和第 4 层信息作为数据包是否转发的条件，也就是能够基于数据包的源地址、目标地址、协议和目标端口这些条件来决定是否转发数据包。这使得扩展访问控制列表比标准访问控制列表的控制粒度更细。

打开随书光盘中第 8 章练习“02 扩展访问控制列表.pkt”，网络拓扑如图 8-5 所示，网络中的路由器和计算机的 IP 地址已经按照网络拓扑中的标识地址配置完成，路由器上已经配置了相应的路由。Router0 是企业内网的路由器，内网有三个网段，Router1 模拟的是 Internet 上的路由器。



▲图 8-5 扩展访问控制列表实验环境

要求	在 Router0 上定义扩展访问控制列表实现以下功能。 允许市场部的计算机能够访问 Internet。 允许财务部的计算机只能访问 Internet 的 10.0.0.0/8 网段的 Web 服务器。 服务器组中的计算机能够 ping 通 Internet 的任何计算机。

操作步骤如下。

（1）在 Router0 上创建扩展访问控制列表。

```
Router>en
Router#config t
Router (config) #access-list 101 permit ip 192.168.2.0 0.0.0.255 any
Router (config) #access-list 101 permit TCP 192.168.1.0 0.0.0.255 10.0.0.0
0.255.255.255 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80) --eq 后面可以是端口或应用层协议名称
Router (config) #access-list 101 permit TCP 192.168.1.0 0.0.0.255 10.0.0.0
0.255.255.255 eq 80
Router (config) #access-list 101 permit icmp 192.168.0.0 0.0.0.255 any
```

扩展访问控制列表的语法：

```
Access-list 编号 {permit | deny} {TCP | UDP } 源地址 目标地址 eq 目标端口
Access-list 编号 {permit | deny} {IP |ICMP } 源地址 目标地址
```

如果协议是 IP 或 ICMP，则后面没有目标端口。

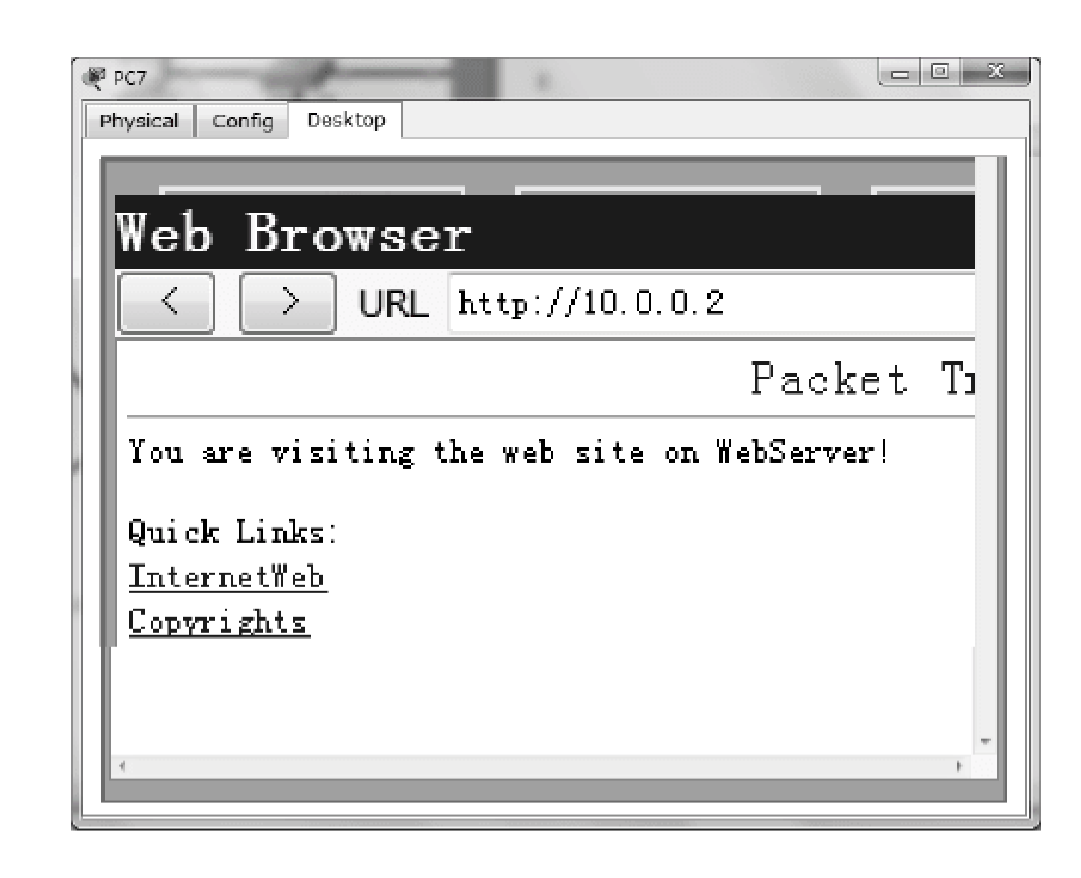
如果你允许了 IP 协议，就等同于允许了所有 TCP、UDP 以及 ICMP 协议的流量。

（2）将扩展访问控制列表绑定到 Router0 的接口。

```
Router (config) #interface Serial 3/0
Router(config-if)#ip access-group 101
out
```

（3）验证扩展访问控制列表的设置。

市场部的计算机 PC7 能够 ping 通 Internet 上任何计算机，也能够访问 WebServer 的网站，如图 8-6 所示。



▲图 8-6 访问 Web 站点

财务部的计算机 PC2 不能 ping 通 Internet

上任何计算机，也能够访问 WebServer 的网站

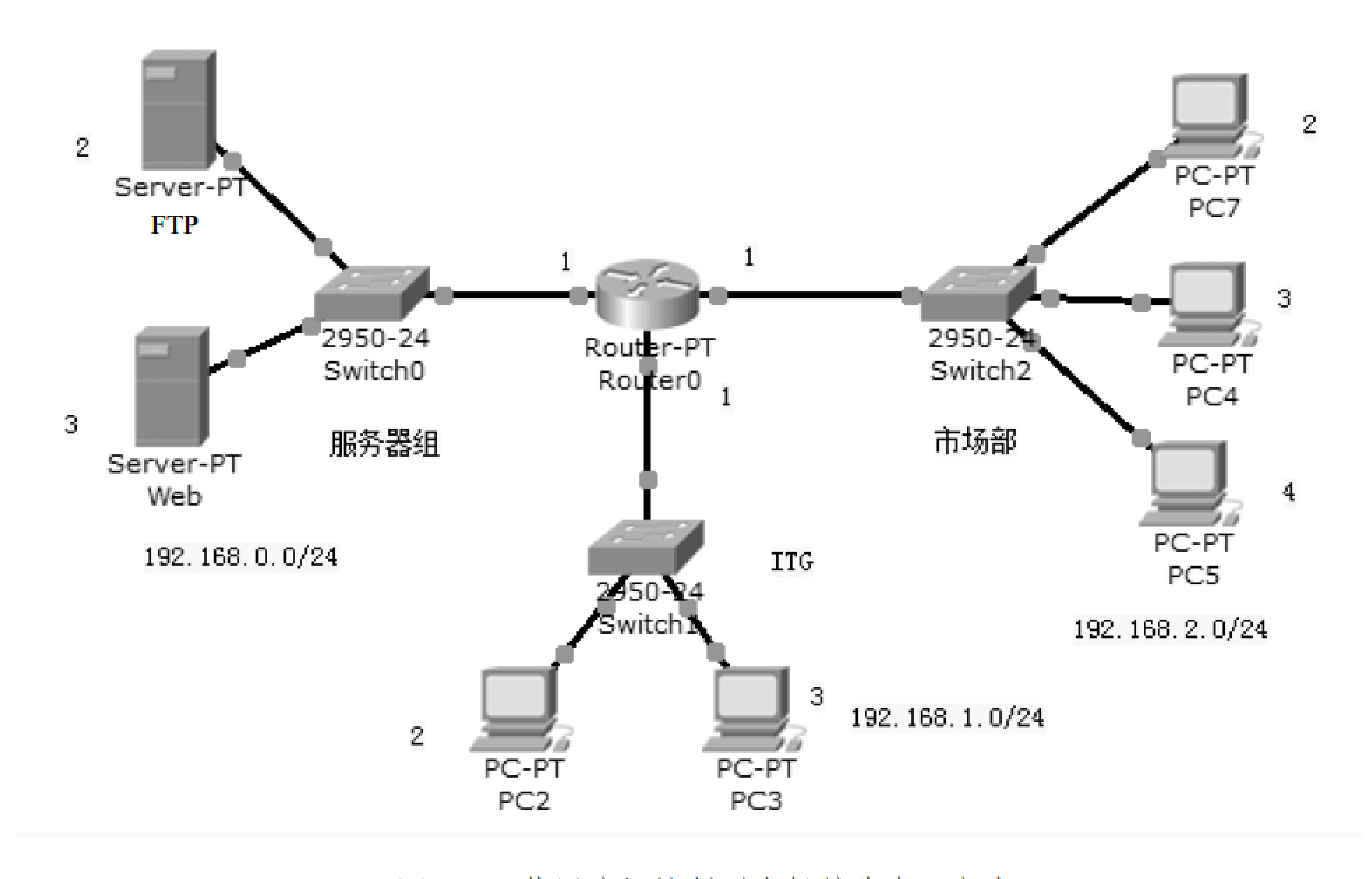
服务器组的计算机能 ping 通 Internet 上任何计算机，但不能访问 WebServer 的网站。

8.2.3 使用访问控制列表保护路由器

为了远程配置路由器方便，路由器一般都开启了 Telnet 功能，如何保护路由器的安全呢？你可以创建访问控制列表只允许特定的计算机能够 Telnet 路由器。路由器的任何一个接口都允许 Telnet，你不得不将访问控制列表应用到每个接口的入口方向上，这对一个具有十几个甚至上百个接口的大型路由器来说不是很好的办法。这里有更好的解决方案：使用标准的 IP 访问列表控制访问 VTY 线路。

打开随书光盘中第 8 章练习“03 使用访问控制列表保护路由器安全.pkt”，网络拓扑如图 8-7 所示，路由器和计算机的 IP 地址已经按照图示的地址配置，且路由器已经配置 Telnet 密码和 enable 密码，分别为 hanlg 和 todd。现在任何一个计算机都可以 Telnet 路由器。

为了安全起见，你需要在 Router0 上创建标准访问控制列表，只允许 ITG 部门的计算机可以 Telnet 路由器。



▲图 8-7 使用访问控制列表保护路由器安全

（1）在 PC7 上 Telnet 路由器，发现只要密码输入正确就能 Telnet 成功。

```
PC>telnet 192.168.2.1
```

（2）在 Router0 上创建标准的访问控制列表。

```
Router(config)#access-list 12 permit 192.168.1.0 0.0.0.255 --定义 ACL
Router(config)#line vty 0 15                               --进入 VTY 虚接口
Router(config-line)#access-class 12 in                     --绑定 ACL
```

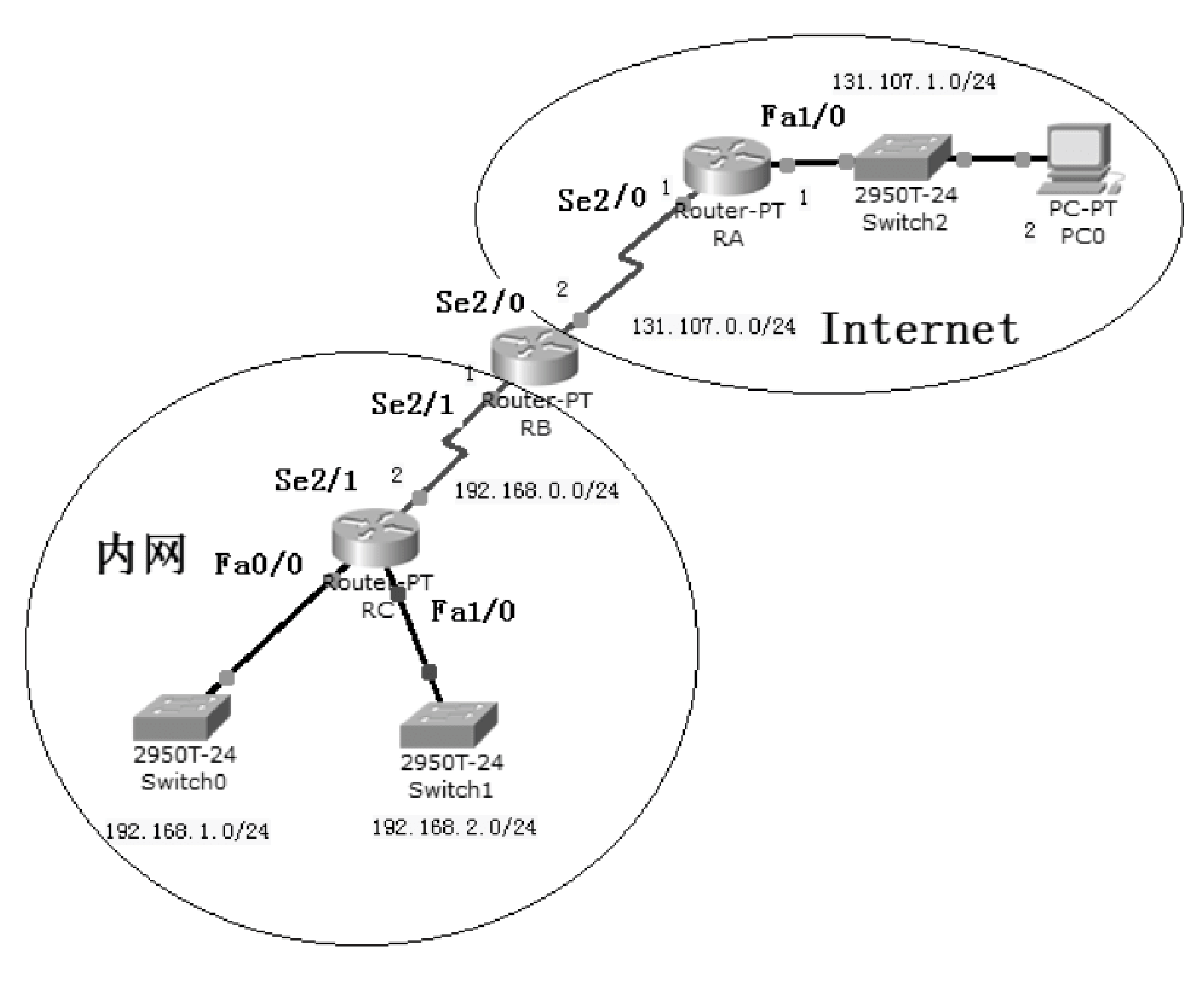
（3）验证只有 ITG 部门的计算机能够 Telnet 到路由器。

```
PC7 telnet 路由器，PC2 telnet 路由器
PC>telnet 192.168.2.1
```

8.3 基于时间的访问控制列表

扩展访问控制列表可以和时间段结合起来过滤流量上网。比如，在路由器上面设置时间段：周一到周五 9:00-12:00 和 14:00-18:00，在这段时间里面员工能访问 Internet，周六和周日只能访问 Internet 的 Web 站点和 DNS 域名解析的流量通过。

基于时间的访问控制列表在 Packet Tracer 软件中的路由器不支持。使用 Dynamips 软件进行基于时间的访问控制列表的实验，路由器 RA、RB 和 RC 的连接如图 8-8 所示。并不是所有的 IOS 都支持基于时间的 ACL，下面的实验中使用 Dynamips 加载了 unzip-c3640-js-mz.124-10.bin 操作系统的虚拟的路由器，按照图示的 IP 地址规划将路由器的接口配置 IP 地址，并且在路由器上添加了路由表，使整个网络是畅通的。RB 模拟的是连接内网和 Internet 的防火墙路由器。以下所有的操作在路由器 RB 上。



▲图 8-8　基于时间的访问控制列表

8.3.1　查看和设置路由器的时间

查看路由器当前的时间，如果不对，应该先配置路由器的时间，然后创建时间段，为访

问控制列表指定时间段。

```
RB#show clock                          --显示路由器上当前时间
10:25:32.955 UTC Mon Nov 15 2010  --当前时间是 2010 年 11 月 15 日 10 点 25 分 32 秒
```

Mon 是 Monday（星期一）的缩写，Nov 是 November（11 月）的缩写，UTC 代表 CoordiNATed Universal Time（协调世界时）。

```
RB#clock set 10:49:23 15 Nov 2010  --将时间设置为 2010 年 11 月 15 日，10 点 49 分
```

8.3.2 定义时间段

如图 8-9 所示，定义一个工作时间段 work-time，周一到周五的 8:00-12:00、14:00-18:00；定义一个 weekend-time，周六、周日全天。

```
RB(config)#time-range work-time
RB(config-time-range)#periodic ?
  Friday      Friday
  Monday      Monday
  Saturday    Saturday
  Sunday      Sunday
  Thursday    Thursday
  Tuesday     Tuesday
  Wednesday   Wednesday
  daily       Every day of the week
  weekdays    Monday thru Friday
  weekend     Saturday and Sunday
RB(config-time-range)#periodic weekdays 8:00 to 12:00
RB(config-time-range)#periodic weekdays 14:00 to 18:00
RB(config-time-range)#exi
```

▲图 8-9　定义时间段

如图 8-10 所示，Weekdays 代表周一到周五，Weekend 代表周六和周日两天。

```
RB(config)#time-range weekend
RB(config-time-range)#periodic weekend 0:00 to 23:59
RB(config-time-range)#exi
```

▲图 8-10　定义时间段

以下命令查看定义的时间段，如图 8-11 所示。

```
RB#show time-range
time-range entry: weekend (inactive)
   periodic weekend 0:00 to 23:59
time-range entry: work-time (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 14:00 to 18:00
```

▲图 8-11　查看定义的时间段

8.3.3 在访问控制列表中使用时间

在创建扩展访问控制列表时可以指定时间创建的时间段。在你指定的时间周期内所涉及的任务功能将会执行，这个时间周期依据路由器的时钟，如图 8-12 所示。

```
RB(config)#access-list 110 permit ip any any time-range work-time
RB(config)#access-list 110 permit TCP any any eq 80 time-range weekend
RB(config)#access-list 110 permit UDP any any eq 53 time-range weekend
```

▲图 8-12 在访问控制列表中使用时间

查看刚才定义的扩展访问控制列表，如图 8-13 所示。

```
RB#show access-lists
Extended IP access list 110
    10 permit ip any any time-range work-time (inactive)
    20 permit tcp any any eq www time-range weekend (inactive)
    30 permit udp any any eq domain time-range weekend (inactive)
```

▲图 8-13 查看定义的访问控制列表

将访问控制列表绑定到接口，如图 8-14 所示。

```
RB(config)#interface serial 2/0
RB(config-if)#ip access-group 110 in
```

▲图 8-14 将访问控制列表绑定到接口

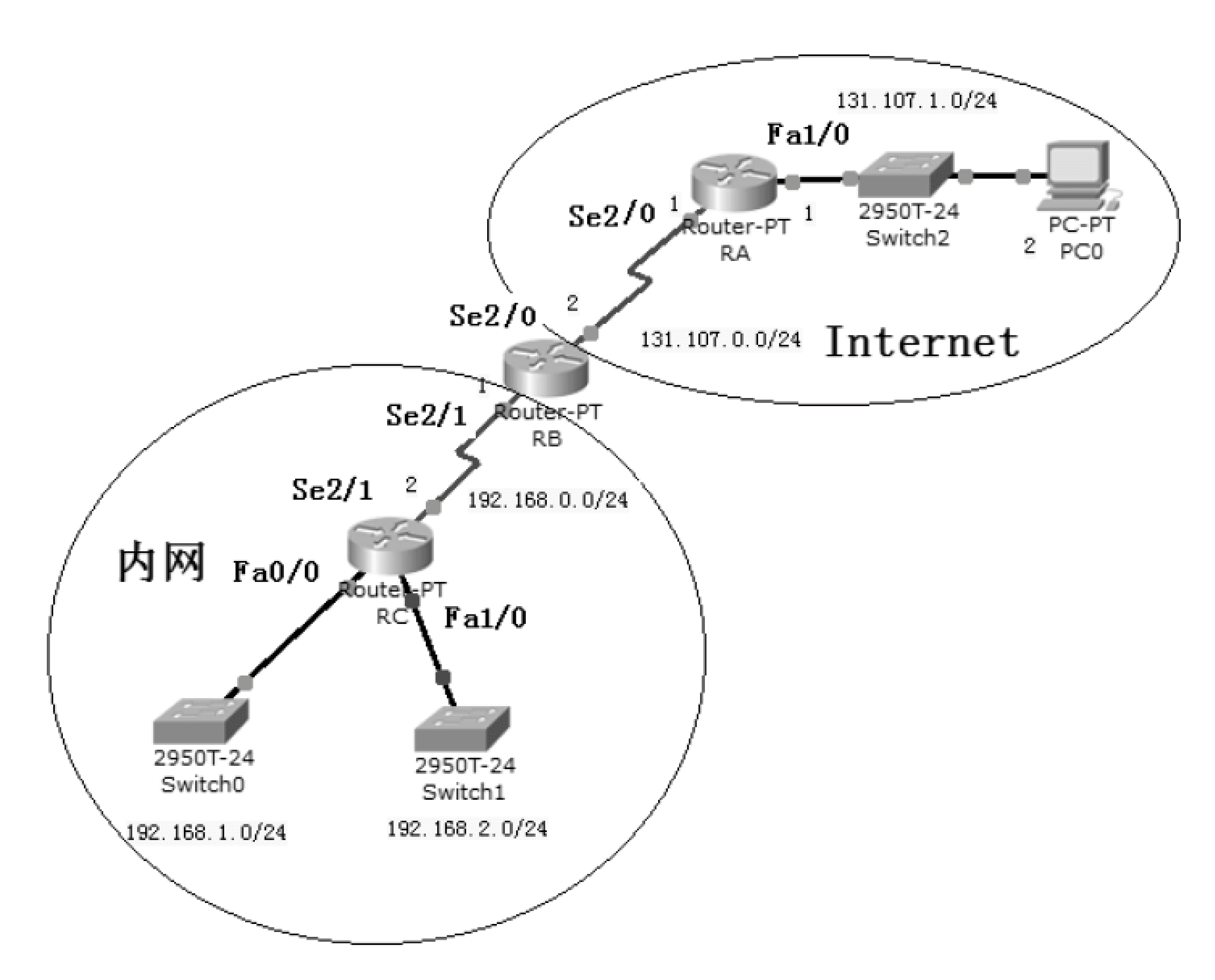
8.4 使用访问控制列表降低安全威胁

下面的实验中使用 Dynamips 加载了 unzip-c3640-js-mz.124-10.bin 操作系统的虚拟的路由器，路由器的网络拓扑如图 8-15 所示，内网有三个网段 192.168.0.0/24、192.168.1.0/24 和 192.168.2.0/24，Internet 用 131.107.0.0/24 和 131.107.1.0/24 两个网段来模拟，路由器 RB 连接 Internet 和内网。网络中路由器的 IP 地址和路由表已经配置完成。运行 Dynamips 软件的虚拟机和 RA 相连，就是图 8-15 中的 PC0。

将在 RB 路由器上配置访问控制列表，用以消除以下威胁。

- IP 地址欺骗——入站；
- IP 地址欺骗——出站；
- DoS TCP SYN 攻击——阻塞外部攻击；
- DoS TCP SYN 攻击——使用 TCP 拦截；
- DoS Smurf 攻击；
- 过滤 ICMP 消息——入站；
- 过滤 ICMP 消息——出站；
- 过滤 ICMP 消息路由跟踪。

以下将会针对每一种网络攻击创建一个访问控制列表，网络拓扑如图 8-15 所示。如果你打算在一个访问控制列表中针对多种网络攻击进行防范，就需要将下面的访问控制列表进行合并，并且需要考虑在访问控制列表中的顺序。

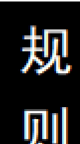


▲图 8-15　访问控制列表降低安全威胁实验环境

8.4.1　IP 地址欺骗对策

攻击者经常用来获取网络信息的一种方法是冒充成一个网络中可信的成员。攻击者欺骗数据包中的源 IP 地址，然后发往内部网络。攻击者只需要将数据包中的源 IP 地址改成一个属于内部子网的地址即可。

1. 入站



规则　决不允许任何源地址是内部主机地址或网络地址的数据包进入一个私有的网络。

```
RB (config) #access-list 150 deny ip 127.0.0.0 0.255.255.255 any log
RB (config) #access-list 150 deny ip 0.0.0.0 255.255.255.255 any log
RB (config) #access-list 150 deny ip 10.0.0.0 0.255.255.255 any log
RB (config) #access-list 150 deny ip 172.16.0.0 0.15.255.255 any log
RB (config) #access-list 150 deny ip 192.168.0.0 0.0.255.255 any log
RB (config) #access-list 150 deny ip 224.0.0.0 15.255.255.255 any log
RB (config) #access-list 150 deny ip host 255.255.255.255 any log
RB (config) #access-list 150 permit ip any any
RB (config) #interface Serial 2/0
RB (config-if) #ip access-group 150 in
```

后面 log 的作用是：当数据包应用该策略被拒绝时将会在控制台显示。

这个访问控制列表拒绝任何来自以下源地址的数据包：

- 任何本地主机地址（127.0.0.0/8）；
- 任何保留的私有地址；
- 任何组播 IP 地址（224.0.0.0/4）。

2. 出站

规则	决不允许任何含有非内部网络有效地址的 IP 数据包出站。

```
RB（config）#access-list 105 permit ip 192.168.0.0 0.0.255.255 any
RB（config）#access-list 105 deny ip any any log
RB（config）#interface Serial 2/0
RB（conofig-if）#ip access-group 105 out
```

8.4.2 DoS TCP SYN 攻击对策

应对 DoS TCP SYN 攻击有两种方法：阻塞外部访问和使用 TCP 拦截。

1. 阻塞外部访问

DoS TCP SYN 攻击会向内部网络发送大量数据包，企图淹没接收结点的连接队列。

```
RB(config)#access-list 109 permit tcp any 192.168.0.0 0.0.255.255 established
RB（config）#access-list 109 deny ip any any log
RB（config）#interface Serial 2/0
RB（config-if）#ip access-group 109 in
```

这个访问控制列表允许来自外部网络的对源自内部网络的请求响应，拒绝任何从外部网络发起的 TCP 连接。

2. 使用 TCP 拦截

TCP 拦截（TCP Intercept）是一种防止内部网络主机遭受外部 TCP SYN 攻击的工具。以下的访问控制列表只允许可达的外部主机发起对内部主机的 TCP 连接，阻塞来自不可达主机的数据包。

```
RB（config）#ip tcp intercept list 110      --在访问控制列表 110 上启用 TCP 拦截
RB（config）#access-list 110 permit tcp any 192.168.0.0 0.0.255.255
RB（config）#access-list 110 deny ip any any log
RB（config）#interface Serial 2/0
```

```
RB（config-if）#ip access-group 110 in
```

TCP 拦截监视 TCP 分组，判断正被请求的连接是否完成。如果 TCP 的连接请求来自一个不可达或者欺骗性的源地址，那么就可能出现拒绝服务（Denial-of-Service，DoS）攻击，目标服务器留下了大量打开一半的连接，最终会耗尽内存。

TCP 拦截能够运行在拦截模式，此时路由器积极地按照这些步骤执行。

（1）路由器拦截来自请求方的 TCP 请求分组。

（2）路由器代表目标服务器向请求方发回一个代理的应答。

（3）路由器等候请求方用它的确认（ACK）跟进。

（4）如果连接的握手进行到此，那么路由器向目标服务器发送原来的请求分组，路由器执行了一次代理的三次握手，就好像目标在和请求方通信一样。

（5）请求方和目标服务器得到许可执行一次正常的 TCP 连接。

拦截模式中，TCP 拦截能够在处于 DoS 攻击而收到大量不完整的连接请求时变得更为主动。主动模式中，每个新的连接请求都会让过去的一次不完整连接被删除。路由器还将重传超时减少一半，并且把等待连接建立的时间减少一半。

TCP 拦截还能够运行在监视模式，此时路由器被动地进行监视，查看是否建立了 TCP 连接。如果在一段超时时间内没有建立连接，那么路由器就向目标服务器发送一个 TCP 复位（RST）信号以清除打开一半的连接。

拦截配制步骤如下。

（1）使用扩展访问控制列表识别 TCP 连接请求。

（2）使用访问控制列表触发 TCP 拦截。

```
(global) ip tcp intercept list acc-list-number
```

（3）设定 TCP 拦截模式，intercept 为主动，watch 为被动。

```
(global) ip tcp intercept mode {intercept|watch}
```

（4）调节 TCP 拦截行为。

设定丢弃模式：oldest，丢弃超时时间最长的（默认）；random，随机丢弃。

```
(global) ip tcp intercept drop-mode {oldest | random}
```

8.4.3 DoS Smurf 攻击对策

Smurf 攻击是向一个路由器子网广播地址，发送大量的 ICMP 包，IP 地址则伪装成属于这个子网。以下例子的目的是防止转发广播，杜绝 Smurf 攻击。

```
RB（config）#access-list 111 deny ip any host 192.168.0.255 log
RB（config）#access-list 111 deny ip any host 192.168.1.255 log
RB（config）#access-list 111 deny ip any host 192.168.2.255 log
RB（config）#access-list 111 deny ip any host 192.168.0.0 log
RB（config）#access-list 111 deny ip any host 192.168.1.0 log
```

```
RB (config) #access-list 111 deny ip any host 192.168.2.0 log
RB (config) #interface Serial 2/0
RB (config-if) #ip access-group 111 in
```

这个 ACL 过滤了所有发往特定广播地址的 IP 数据包。

8.4.4 过滤 ICMP 消息

1. 入站

ICMP Echo 数据包可用来发现子网和受保护网络中的主机，也能用来实施 DoS 攻击。ICMP 重定向消息可用来更改主机路由选择表。无论是 ICMP Echo 还是重定向消息，都应该被路由器做入站阻塞。

```
RB (config) #access-list 112 deny icmp any any echo log
RB (config) #access-list 112 deny icmp any any redirect log
RB (config) #access-list 112 deny icmp any any mask-request log
RB (config) #access-list 112 permit icmp any 192.168.0.0 0.0.255.255
RB (config) #interface Serial 2/0
RB (config) #ip access-group 112 in
```

2. 出站

下列 ICMP 消息用作网管，应该允许出站。

- 回声（Echo）：允许用户 ping 外部主机；
- 参数问题（Parameter problem）：通知主机数据包头问题；
- 数据包太大（Packet too big）：需要 MTU 发现；
- 源队列（Source quench）：必要时遏制流量。

应该阻止其他 ICMP 消息出站。

```
RB (config) #access-list 114 permit icmp 192.168.0.0 0.0.255.255 any echo
RB ( config ) #access-list 114 permit icmp 192.168.0.0 0.0.255.255 any parameter-problem
RB ( config ) #access-list 114 permit icmp 192.168.0.0 0.0.255.255 any packet-too-big
RB ( config ) #access-list 114 permit icmp 192.168.0.0 0.0.255.255 any source-quench
RB (config) #access-list 114 deny icmp any any log
RB (config) #interface Serial 2/0
RB (config-if) #ip access-group 114 out
```

3. 路由跟踪

路由跟踪（traceroute）特性是通过一些 ICMP 消息类型来实现的。路由跟踪会显示数据包从源到目的地所经过的路由器结点的 IP 地址。攻击者可以利用对路由跟踪 ICMP 消息的响应来刺探子网和受保护网络的主机。

应该阻止所有入站和出站的路由跟踪 UDP 消息。

```
RB（config）#access-list 120 deny udp any any range 33400 34400 log
RB（config）#interface serial 2/1
RB（config-if）#ip access-group 120 in
RB（config）#access-list 121 permit udp 192.168.0.0 0.0.255.255 any range 33400 34400 log
RB（config）#interface serial 2/0
RB（config-if）#ip access-group 121 in
```

8.4.5 DDoS 对策

1. TRIN00

下面例子演示了如何阻塞 TRIN00 DDoS 攻击。需要阻塞的端口流量如下。

```
TCP——1524（Ingress Lock）
TCP——27665（未分配）
UDP——31335（未分配）
UDP——27444（未分配）
RB（config）#access-list 190 deny tcp any any eq 1524 log
RB（config）#access-list 190 deny tcp any any eq 27665 log
RB（config）#access-list 190 deny udp any any eq 31335 log
RB（config）#access-list 190 deny udp any any eq 27444 log
```

2. Stacheldraht

下面例子演示了如何阻塞 Stacheldraht DDoS 攻击。需要阻塞的端口流量如下。

```
TCP——16660（未分配）
TCP——65000（未分配）
RB（config）#access-list 190 deny tcp any any eq 16660 log
RB（config）#access-list 190 deny tcp any any eq 65000 log
```

Stacheldraht DDoS 用 ICMP Echo 请求和 Echo 响应消息建立通信，并且控制和监视攻击。通过阻塞 TCP 端口 16660 和 65000 可以阻止实际的攻击，但如果想防止攻击者在系统上设置后门，还应该设法阻塞 ICMP Echo 请求（TCP 端口 8）和 ICMP Echo 响应（TCP 端口 0），

命令如下：

```
RB (config) #access-list 190 deny icmp any any echo
RB (config) #access-list 190 deny icmp any any echo-reply
```

> **注意** 阻塞了这些 ICMP 端口，会影响使用 ping 命令，这可能是不希望看到的。

3. Trinity V3

下面例子演示了如何阻塞 Trinity V3 DDoS 攻击。需要阻塞的端口流量如下。

```
TCP——33270（未分配）
TCP——39168（未分配）
RB (config) #access-list 190 deny tcp any any eq 33270 log
RB (config) #access-list 190 deny tcp any any eq 39168 log
```

4. Subseven

下面例子演示了如何阻塞 Subseven DDoS 攻击。需要阻塞的端口流量如下。

```
TCP——范围从 6711～6712（未分配）
TCP——6776（未分配）
TCP——6669（IRCU）
TCP——2222（Rockwell CSP1）
TCP——7000（AFS2 Fileserver）
RB (config) #access-list 190 deny tcp any any range 6711 6712 log
RB (config) #access-list 190 deny tcp any any eq 6776 log
RB (config) #access-list 190 deny tcp any any eq 6669 log
RB (config) #access-list 190 deny tcp any any eq 2222 log
RB (config) #access-list 190 deny tcp any any eq 7000 log
```

8.5 访问控制列表的位置

将 IP 标准访问控制列表尽可能放置在靠近目的地址的位置，这是因为我们并不真正的要在自己的网络内使用表中的访问控制列表。不能将标准访问控制列表放置在靠近源主机或源网络的位置，因为这样会过滤基于源地址的流量，而导致不能转发任何流量。

将扩展访问控制列表尽可能放置在靠近源地址的位置。既然扩展访问控制列表可以过滤每个特定的地址和协议，那么我们就不希望流量穿过整个网络后再被拒绝。通过将这样的列表放置在尽量靠近源地址的位置，可以在它使用有限的带宽之前过滤掉此流量。

8.6 习 题

1. 路由器的访问控制列表的作用是________。
   A. 访问控制列表可以监控交换的字节数
   B. 访问控制列表提供路由过滤功能
   C. 访问控制列表可以检测网络病毒
   D. 访问控制列表可以提高网络的利用率
2. 以下的访问控制列表中，________禁止所有 Telnet 访问子网 10.10.1.0/24。
   A. access-list 15 deny telnet any 10.10.1.0 0.0.0.255 eq 23
   B. access-list 1 15 deny udp any 10.10.1.0 eq telnet
   C. access-list 115 deny tcp any 10.10.1.0 0.0.0.255 eq 23
   D. access-list 15 deny udp any 10.10.1.0 255.255.255.0 eq 23
3. ________IP 地址和反转掩码可以用来阻断来自 192.168.16.43/28 网段的流量。
   A. 192.168.16.32 0.0.0.16
   B. 192.168.16.43 0.0.0.212
   C. 192.168.16.0 0.0.0.15
   D. 192.168.16.32 0.0.0.15
   E. 192.168.16.0 0.0.0.31
   F. 192.168.16.16 0.0.0.31
4. 一个标准访问控制列表应用到路由器的一个以太网接口，该标准访问控制列表能够基于______来过滤流量。
   A. 源地址和目标地址
   B. 目标端口
   C. 目标地址
   D. 源地址
   E. 以上所有
5. 河北师大软件学院某个子网使用 29 位的子网掩码，在配置扩展访问控制列表时如何允许或拒绝整个子网？________
   A. 255.255.255.224
   B. 255.255.255.248
   C. 0.0.0.224
   D. 0.0.0.8
   E. 0.0.0.7
   F. 0.0.0.3
6. 假若你是石家庄飞烨科技公司的网络管理员，你正打算使用访问控制列表到路由器

的一个接口，_______命令可以达到目的。

A. permit access-list 101 out

B. ip access-group 101 out

C. apply access-list 101 out

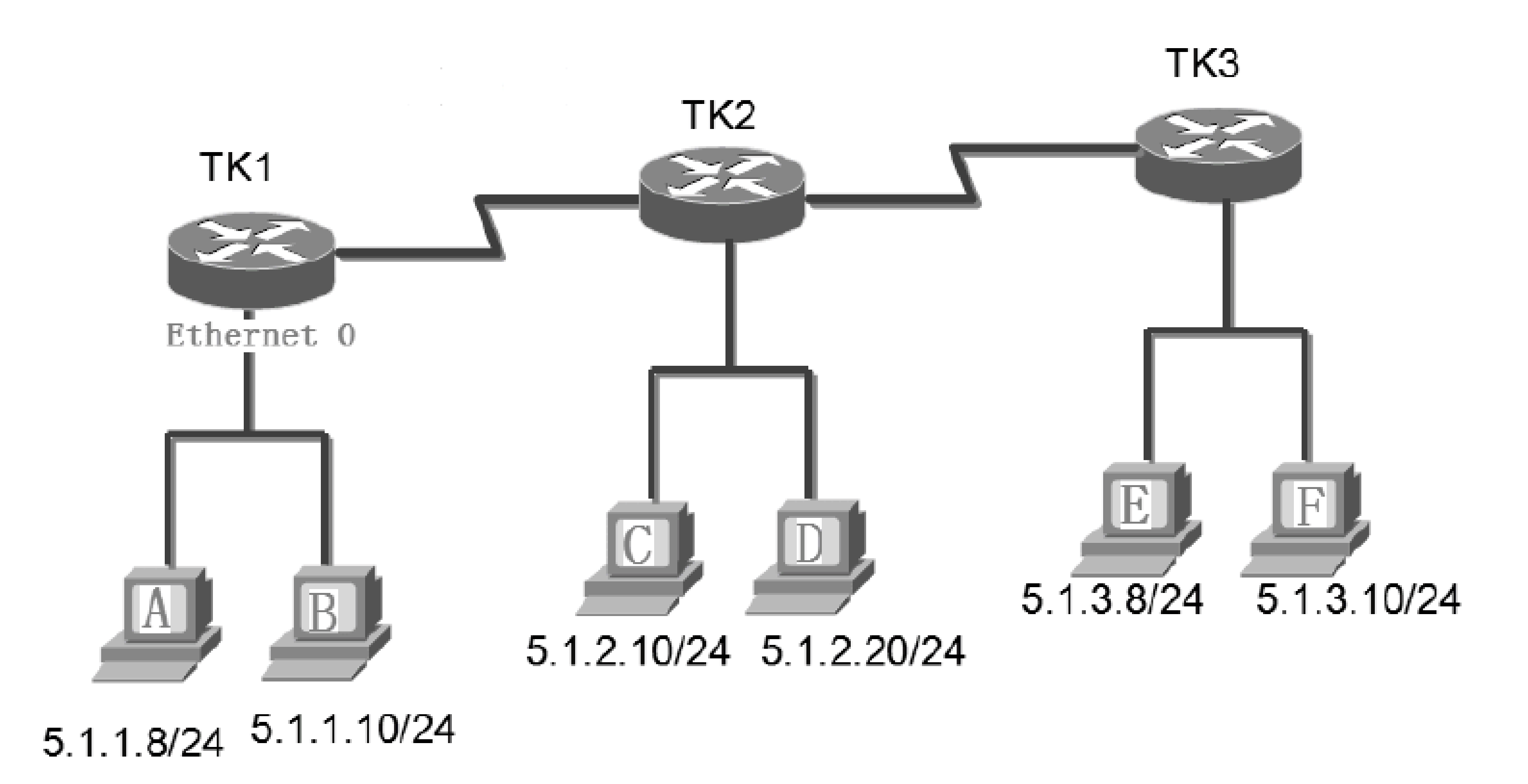
D. access-class 101 out

E. ip access-list e0 out

7. 石家庄新迈科技公司网络拓扑如图 8-16 所示。你是公司的系统管理员，在 TK1 路由器上，你定义了以下访问控制列表。

Access-list 101 deny tcp 5.1.1.10 0.0.0.0 5.1.3.0 0.0.0.255 eq telnet

Access-list 101 permit ip any any



▲图 8-16　网络拓扑

你将该访问控制列表绑定到 TK1 的 Ethernet 0 接口，ip access-group 101 in，_______将会被访问控制列表阻断。

A. 从主机 A 访问主机 5.1.1.10 的 Telnet 会话

B. 从主机 A 访问主机 5.1.3.10 的 Telnet 会话

C. 从主机 B 访问主机 5.1.2.10 的 Telnet 会话

D. 从主机 B 访问主机 5.1.3.8 的 Telnet 会话

E. 从主机 C 访问主机 5.1.3.10 的 Telnet 会话

8. 在路由器的串口，一个入站的访问控制列表配置拒绝 TCP 端口 21、 23 和 25，所有的其他流量允许。基于这个信息，_____类型的流量将会被允许通过该接口。（选择 3 个）

A. SMTP

B. DNS

C. FTP

D. Telnet

E. HTTP

F. POP3

9. ________命令可以将一个访问控制列表绑定到路由器的 VTY 接口。

A. RouterTK（config-line）# access-class 10 in

B. RouterTK（config-if）# ip access-class 23 out

C. RouterTK（config-line）# access-list 150 in

D. RouterTK（config-if）# ip access-list 128 out

E. RouterTK（config-line）# access-group 15 out

F. RouterTK（config-if）# ip access-group 110 in

10. 实施访问控制列表通常的指导方针是________。

A. 应该放置标准访问控制列表尽可能靠近源网络

B. 应该放置扩展访问控制列表尽可能接近源网络

C. 应该放置标准访问控制列表尽可能接近目标网络

D. 应该放置扩展访问控制列表尽可能接近目标网络

习题答案

1．B

2．C

3．D

4．D

5．E

6．B

7．D

8．B、E、F

9．A

10．B、C

第 9 章　网络地址转换

本章将介绍网络地址转换（Network Address Translation，NAT）、动态网络地址转换和端口地址转换（Port Address Translation，PAT），PAT 也称为复用；将会介绍 NAT、PAT 和端口映射的应用场景以及配置方法。

同时也演示了使用 Windows XP 配置连接共享实现 NAT 和端口映射，在 Windows Server 2003 上配置 NAT 和端口映射。

本章主要内容：

- 应用 NAT 的场景
- 配置静态 NAT
- 配置动态 NAT
- 配置 PAT
- 配置端口映射
- 通过 Internet 连接共享配置 NAT 和端口映射
- 通过配置 Windows Server NAT 实现地址转换和端口映射

9.1 网络地址转换技术简介

下面介绍 NAT 的应用场景、NAT 的优缺点以及 NAT 的三种类型。

9.1.1 NAT 的应用场景

NAT 的最初目的是允许将私有 IP 地址映射到公网（合法的 Internet IP 地址）地址的，以减缓 IP 地址空间的消耗。

当一个组织更换它的互联网服务提供商（Internet Service Provider，ISP），比如从网通更改为电信，如果不想更改内网配置方案时，NAT 同样很有用途。

以下是符合使用 NAT 的各种情况。

- 需要连接 Internet，但是你的主机没有公网 IP 地址。
- 更换了一个新的 ISP，需要重新组织网络。
- 需要合并两个具有相同网络地址的内网。

NAT 一般应用在边界路由器中，比如公司连接 Internet 的路由器上。NAT 的优缺点如表 9-1 所示。

表 9-1　NAT 的优点和缺点

优　点	缺　点
节约合法的公网 IP 地址	地址转换产生交换延迟，也就是消耗路由器性能
减少地址重叠出现	无法进行端到端的 IP 跟踪
增加连接 Internet 的灵活性	某些应用无法在 NAT 的网络中运行
增加内网的安全性	

NAT 最显著的优点是节约你的合法公网 IP 地址，正是因为这个原因我们到现在还能使用 IPv4，否则早已升级到 IPv6 了。

9.1.2 NAT 的类型

下面介绍 NAT 的三种类型：静态 NAT、动态 NAT 和 PAT。

- 静态 NAT：这种类型的 NAT 是为了在本地和全球地址间允许一对一映射而设计的。需要记住的是，静态 NAT 需要网络中的每台主机都拥有一个真实的因特网 IP 地址，多用于公网地址到内网主机的端口映射。
- 动态 NAT：这种类型的 NAT 可以实现映射一个未注册 IP 地址到注册 IP 地址池中的一个注册 IP 地址。你不必像使用静态 NAT 那样，在路由器上静态映射内部到外部的地址，但是你必须保证拥有足够的真实 IP，保证每个在因特网中收发包的用户

都有真实的 IP 可用。

- PAT：这是最流行的 NAT 配置类型。PAT 实际上是动态 NAT 的一种形式，它映射多个私网 IP 地址到一个公网 IP 地址，通过使用不同的端口来区分内网主机，也被称为复用。通过使用 PAT，可实现上千个用户仅通过一个真实的全球 IP 地址连接到 Internet。使用复用是我们至今在互联网上没有使用完合法 IP 地址的真实原因。

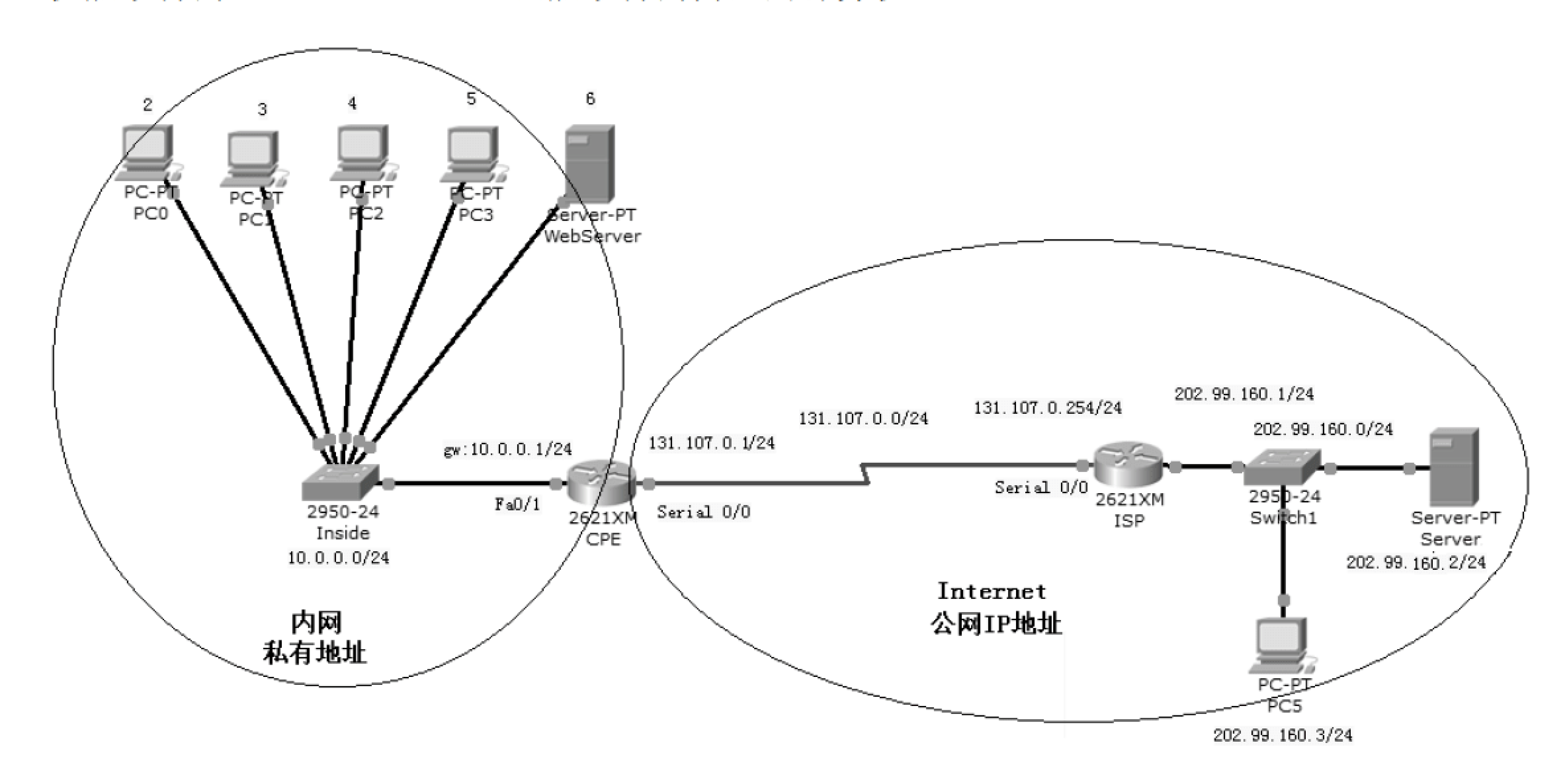
9.2 实现网络地址转换

下面介绍各种类型网络地址转换的实现过程，以及配置步骤。

9.2.1 配置静态 NAT

这种类型的 NAT 是为了在本地和全球地址间允许一对一映射而设计的。需要记住的是，静态 NAT 需要网络中的每台主机都拥有一个真实的因特网 IP 地址，多用于公网地址到内网主机的端口映射。

打开随书光盘中第 9 章练习“01 配置静态 NAT.pkt”，网络拓扑如图 9-1 所示。网络中的计算机和路由器已经配置好了 IP 地址和路由表，企业内网使用私有 IP 地址 10.0.0.0/24，CPE 是连接 Internet 和内网的边界路由器，你需要在 CPE 上配置静态 NAT，使内网的计算机能够访问 Internet，Internet 也能够访问内网的计算机。



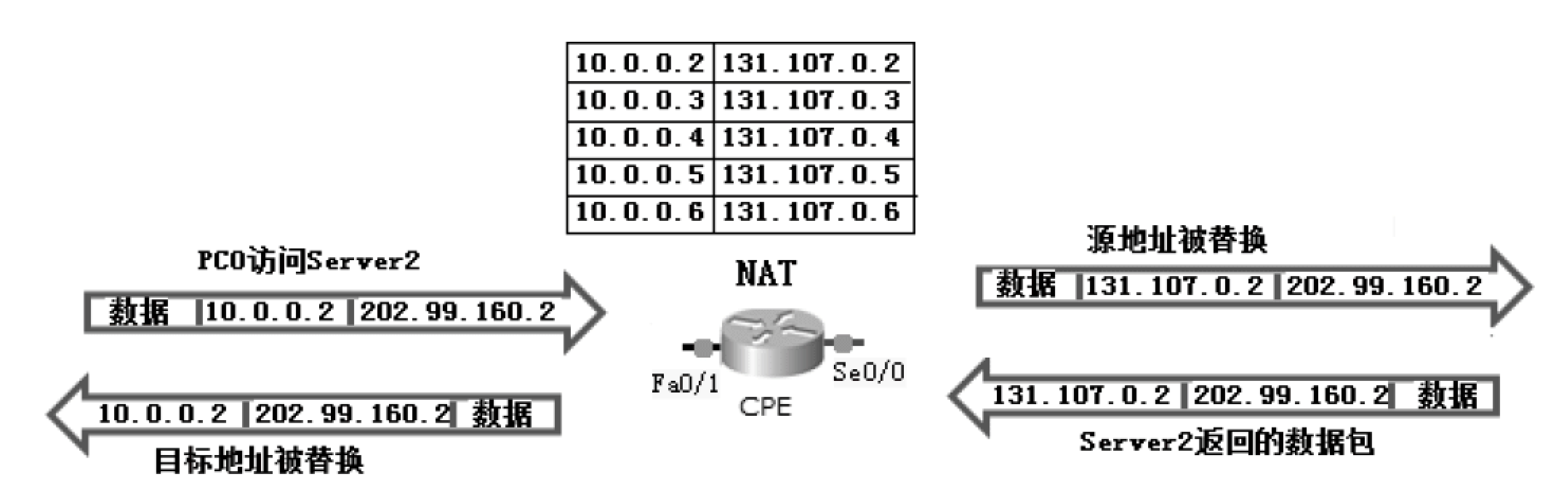
▲图 9-1 静态 NAT 实验环境

在路由器 CPE 上配置静态 NAT 映射。

- 内网计算机 PC0 的私网地址 10.0.0.2 使用公网地址 131.107.0.2 地址。

- 内网计算机 PC1 的私网地址 10.0.0.3 使用公网地址 131.107.0.3 地址。
- 内网计算机 PC2 的私网地址 10.0.0.4 使用公网地址 131.107.0.4 地址。
- 内网计算机 PC3 的私网地址 10.0.0.5 使用公网地址 131.107.0.5 地址。
- 内网计算机 WebServer 的私网地址 10.0.0.6 使用公网地址 131.107.0.6 地址。

如图 9-2 所示，是配置了静态映射路由器，数据包传输过程中的数据包转换。



▲图 9-2　静态 NAT 映射数据包转换过程

配置了静态映射后，PC0 访问 Internet 的 Server，数据包经过 CPE 路由器，根据配置的静态映射，数据包的源地址被 131.107.0.2 地址替换。

Server 向 131.107.0.2 发送返回的数据包，在进入内网时，根据配置的静态映射表，将会使用 PC0 的 IP 地址替换数据包的目标地址。

配置静态映射的步骤如下。

（1）验证配置静态映射前内网的计算机不能和 Intenret 上的计算机通信。PC0 ping 202.99.160.2 不通。

（2）在 CPE 上配置静态 NAT 映射。

```
CPE>en
CPE#config t
CPE（config）#ip NAT inside source static 10.0.0.2 131.107.0.2
CPE（config）#ip NAT inside source static 10.0.0.3 131.107.0.3
CPE（config）#ip NAT inside source static 10.0.0.4 131.107.0.4
CPE（config）#ip NAT inside source static 10.0.0.5 131.107.0.5
CPE（config）#ip NAT inside source static 10.0.0.6 131.107.0.6
CPE（config）#interface fastEthernet 0/1
CPE（config-if）#ip NAT inside          --指定该接口为 NAT 的内网接口
CPE（config-if）#ex
CPE（config）#int
CPE（config）#interface Serial 0/0
CPE（config-if）#ip NAT outside         --指定该接口为 NAT 的外网接口
```

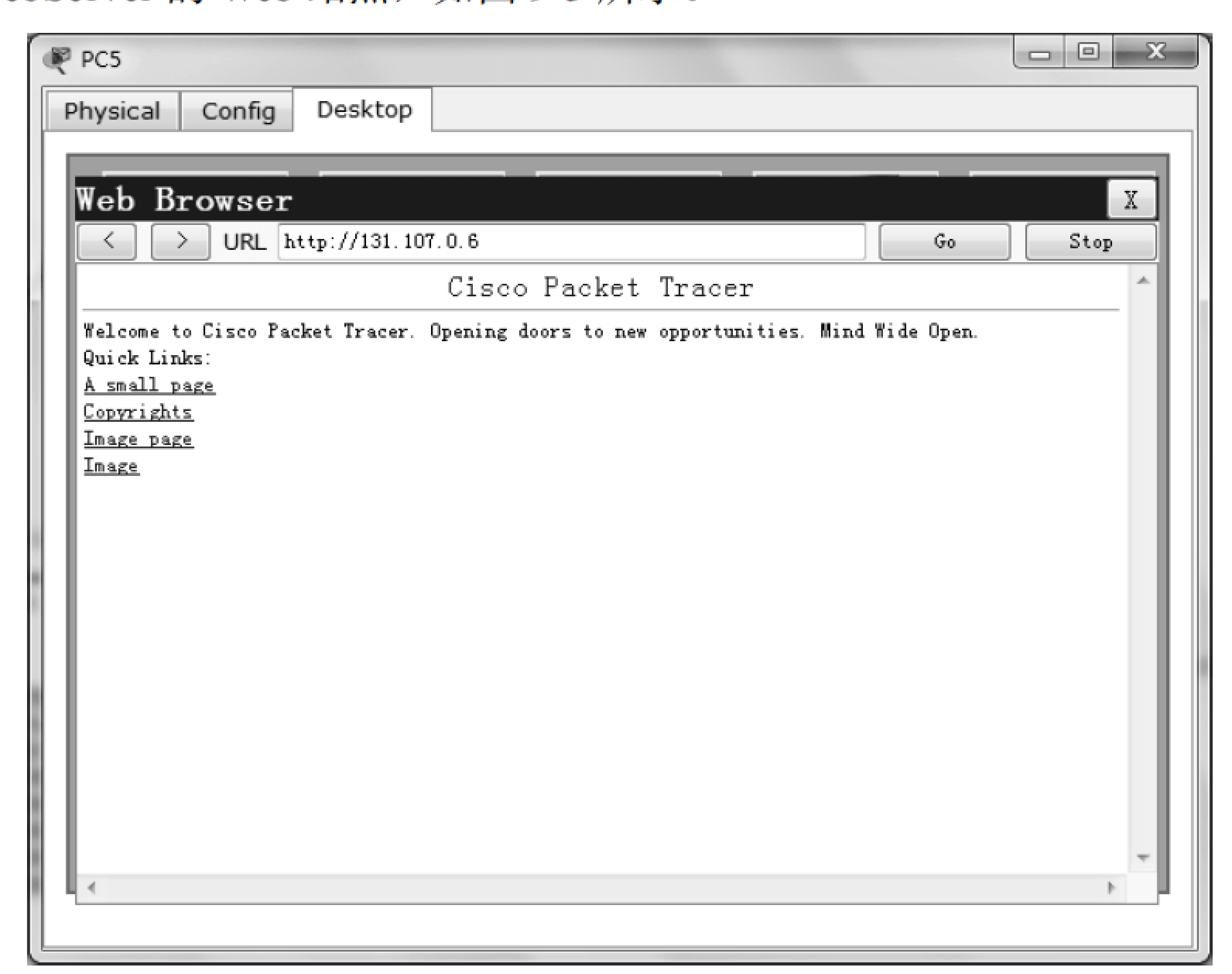
```
CPE (config-if) #ex
CPE#debug ip NAT                          --让路由器显示 NAT 信息
```

（3）验证配置了静态映射后，内网计算机能够访问 Internet。PC0 ping 202.99.160.2 能够通。

（4）在 CPE 路由器上的显示如下。

```
CPE#
NAT: s=10.0.0.2->131.107.0.2, d=202.99.160.2 [1]
NAT*: s=202.99.160.2, d=131.107.0.2->10.0.0.2 [1]
```

（5）配置了静态映射后，Internet 上的计算机通过访问 131.107.0.6 能够访问内网的 WebServer 的 Web 站点，如图 9-3 所示。

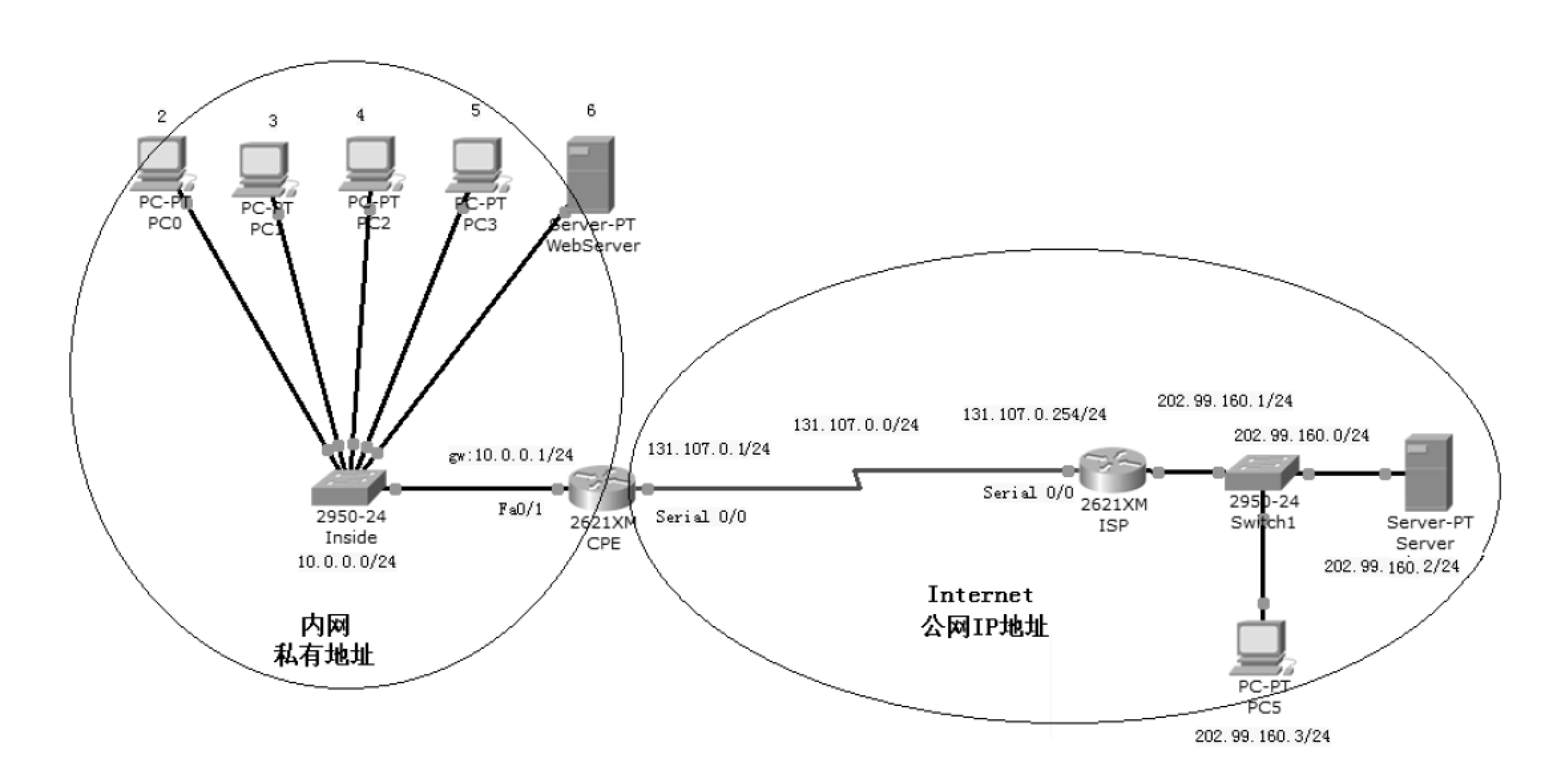


▲图 9-3　验证静态映射

9.2.2　配置动态 NAT

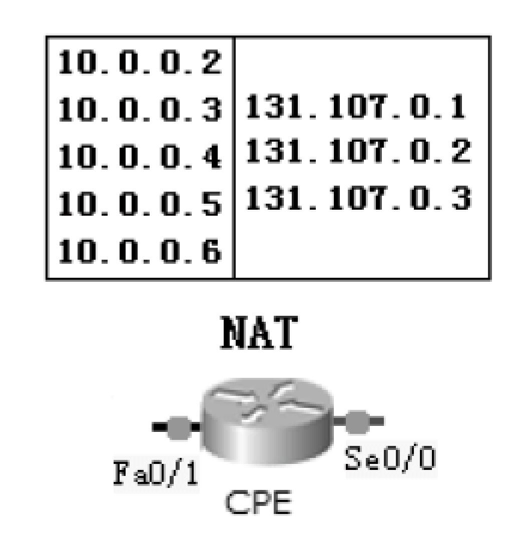
这种类型的 NAT 可以实现映射一个未注册 IP 地址到注册 IP 地址池中的一个注册 IP 地址。你不必像使用静态 NAT 那样，在路由器上静态映射内部到外部的地址，但是你必须保证拥有足够的真实 IP，保证每个在因特网中收发包的用户都有真实的 IP 可用。

打开随书光盘中第 9 章练习“02 动态 NAT.pkt”，网络拓扑如图 9-4 所示。网络中的计算机和路由器已经配置好了 IP 地址和路由表，企业内网使用私有 IP 地址 10.0.0.0/24，CPE 是连接 Internet 和内网的边界路由器，你需要在 CPE 上配置动态 NAT，使内网的计算机能够访问 Internet。注意，动态 NAT，Internet 上的计算机不能访问内网上的计算机。



▲图 9-4　动态 NAT 实验环境

如图 9-5 所示，本实验外网地址有 3 个地址，内网有 5 台计算机，配置为动态映射，只有 3 个内网的计算机能够做地址转换。也就是内网的计算机同时只能有 3 台计算机访问 Internet。（这可是我故意这样设计的）



▲图 9-5　动态 NAT 映射

配置动态 NT 的步骤如下。

（1）在 CPE 上配置动态 NAT。

```
CPE#config t
CPE（config）#access-list 10 permit 10.0.0.0 0.0.0.255
```

定义访问控制列表，如果内网有多个网段需要 NAT，则需要在 ACL 中都添加上。

```
CPE（config）#ip NAT pool todd 131.107.0.1 131.107.0.3 netmask 255.255.255.0
```

todd 是地址池的名字，可以任意指定。指定公网地址池的开始地址和结束地址，以及子网掩码，地址池只有 3 个地址，也就是说只允许内网的 3 个计算机能够访问 Internet。

```
CPE（config）#ip NAT inside source list 10 pool todd    --地址池和访问控制列表进行关联
CPE（config）#interface Serial 0/0
```

```
CPE（config-if）#ip NAT outside                    --指定 NAT 的外网接口
CPE（config-if）#ex
CPE（config）#interface fastEthernet 0/1
CPE（config-if）#ip NAT inside                     --指定 NAT 的内网接口
```

（2）在 CPE 上查看 NAT 配置的状态。

```
CPE#show ip NAT statistics
Total translations: 0 （0 static, 0 dynamic, 0 extended）
Outside Interfaces: Serial0/0
Inside Interfaces: fastEthernet0/1
Hits: 13  Misses: 20
Expired translations: 13
Dynamic mappings:                                  --动态映射
-- Inside Source
access-list 10 pool todd refCount 0
 pool todd: netmask 255.255.255.0
      start 131.107.0.1 end 131.107.0.3
      type generic, total addresses 3 , allocated 0 （0%）, misses 3
```

（3）使用 PC0 访问 Server 的 Web 站点，用 PC1、PC2 和 PC3 ping Server。将发现 PC0 能够访问 Server 的 Web 站点，PC1 和 PC2 能够 ping 通 Server，PC3 却不能 ping 通 Server。那是因为地址池仅 3 个地址，只允许三个内网的主机访问外网。

（4）查看 NAT 地址转换信息。

```
CPE#show ip NAT translations
Pro  Inside global      Inside local       Outside local       Outside global
icmp 131.107.0.2:5      10.0.0.3:5         202.99.160.3:5      202.99.160.3:5
icmp 131.107.0.2:6      10.0.0.3:6         202.99.160.3:6      202.99.160.3:6
tcp  131.107.0.1:1025  10.0.0.2:1025     202.99.160.2:80     202.99.160.2:80
tcp  131.107.0.1:1026  10.0.0.2:1026     202.99.160.2:80     202.99.160.2:80
tcp  131.107.0.1:1027  10.0.0.2:1027     202.99.160.2:80     202.99.160.2:80
```

（5）清除转换表中的 NAT 条目。

```
CPE#clear ip NAT translation *
```

（6）PC3 ping Server，能通。

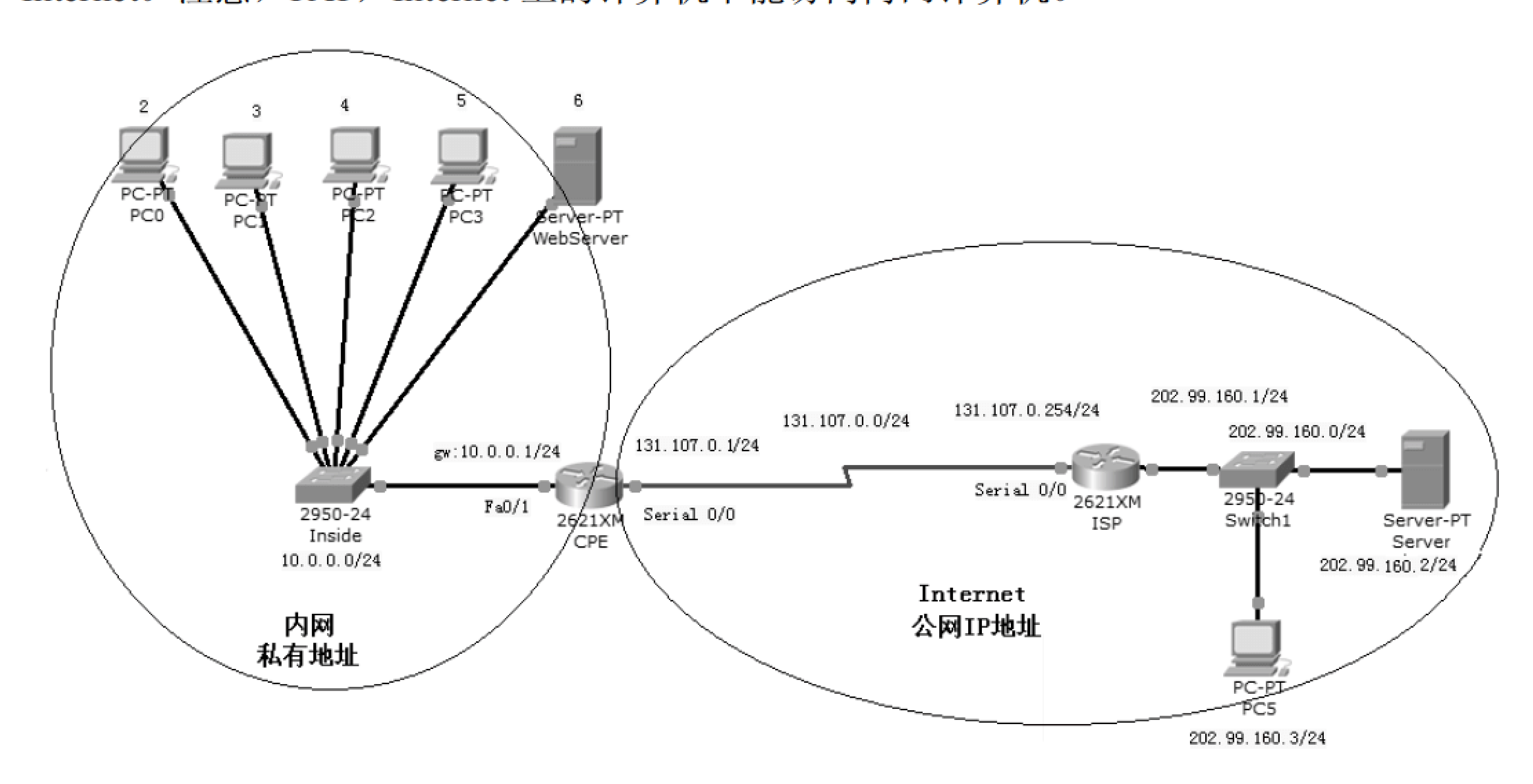
总结

使用动态 NAT 技术，如果地址池的 IP 地址做映射用完了，剩余的内网的计算机将不能再访问外网。

9.2.3 配置 PAT

这是最流行的 NAT 配置类型。PAT 实际上是动态 NAT 的一种形式，它映射多个私网 IP 地址到一个公网 IP 地址，通过使用不同的端口来区分内网主机，也被称为复用。通过使用 PAT，可实现上千个用户仅通过一个真实的全球 IP 地址连接到 Internet。使用复用是我们至今在互联网上没有使用完合法 IP 地址的真实原因。

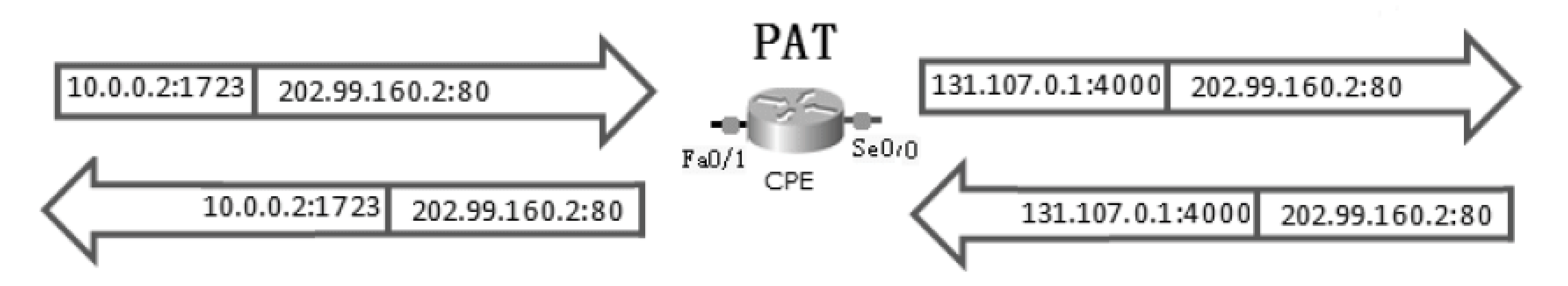
打开随书光盘中第 9 章练习“03 PAT.pkt”，网络拓扑如图 9-6 所示。网络中的计算机和路由器已经配置好了 IP 地址和路由表，企业内网使用私有 IP 地址 10.0.0.0/24，CPE 是连接 Internet 和内网的边界路由器，你需要在 CPE 上配置 PAT，使内网的计算机能够访问 Internet。注意，PAT，Internet 上的计算机不能访问内网计算机。



▲图 9-6　PAT 实验环境

如图 9-7 所示，PC0 访问 Internet 上的 Server 的 Web 站点，源端口可能是 1723，PC1 访问 Internet 上的 Server 的 Web 站点，源端口也可能是 1723，如果数据包只做地址转换，返回的数据包目标地址都是 131.107.0.1、目标端口都是 1723，路由器就没有办法确定这个数据包应该发送给 PC0 还是 PC1。因此如果使用一个公网 IP 地址让很多内网计算机访问 Internet，必须由路由器对访问 Internet 的数据包进行统一的源端口替换，如图 9-7 所示，使用不同的源端口进行替换，这样路由器就可以根据返回的数据包目标端口确定数据包应该转发给哪一个内网的计算机。

	协议	内网地址和端口	外网地址和端口	Server地址和端口
PC0 访问 Server	TCP	10.0.0.2:1723	131.107.0.1:4000	202.99.160.2:80
PC1 访问 Server	TCP	10.0.0.3:1723	131.107.0.1:4001	202.99.160.2:80
PC2访问 Server	TCP	10.0.0.4:1723	131.107.0.1:4002	202.99.160.2:80
PC3 访问 Server	TCP	10.0.0.5:1723	131.107.0.1:4003	202.99.160.2:80



▲图 9-7　源端口替换

配置 PAT 的步骤如下。

（1）在 CPE 上配置 PAT。

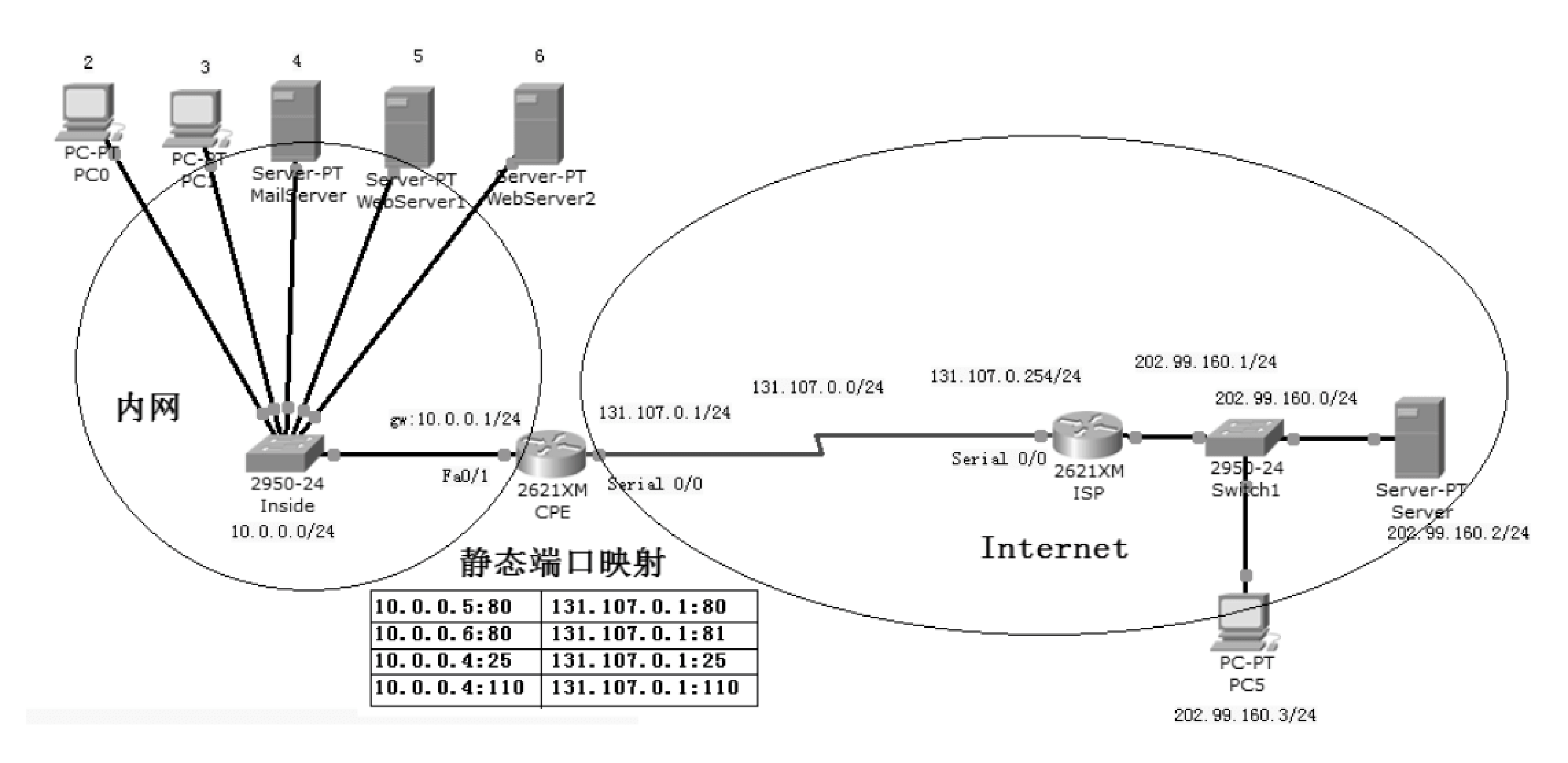
```
CPE#config t
CPE（config）#access-list 10 permit 10.0.0.0 0.0.0.255
CPE（config）#ip NAT pool todd 131.107.0.1 131.107.0.1 netmask 255.255.255.0
                                       --前后两个地址一样，因为就一个公网地址
CPE（config）#ip NAT inside source list 10 pool todd  overload
                                       --overload 参数将会启用 PAT
CPE（config）#interface Serial 0/0
CPE（config-if）#ip NAT outside        --指定 NAT 的外网接口
CPE（config-if）#ex
CPE（config）#interface fastEthernet 0/1
CPE（config-if）#ip NAT inside        --指定 NAT 的内网接口
```

（2）使用 PC0、PC1、PC2、PC3 和 WebServer ping Internet 上的 Server，都能通。

9.2.4　配置端口映射

端口映射是应用非常广泛的技术，很多单位只有一个公网 IP 地址，通过配置 PAT 允许内网的计算机使用这个公网 IP 地址访问 Internet，同时还可以配置静态的端口映射，使得 Internet 上的用户访问内网的服务器。如下面的实验，内网有两个 Web 服务器，可以将公网地址 131.107.0.1 的 TCP 协议 80 端口映射到内网的 WebServer1，将公网地址 131.107.0.1 的 TCP 协议 81 端口映射到内网的 WebServer2。通过将公网地址的 TCP 的 25 端口和 TCP 的 110 端口映射到内网的邮件服务，可以使 Internet 用户访问内网的邮件服务器。

打开随书光盘中第 9 章练习“04 端口映射.pkt”，网络拓扑如图 9-8 所示。网络中的路由器和计算机已经配置好了 IP 地址，你需要在 CPE 路由器上配置端口映射，使 Internet 上的用户能够访问内网的 MailServer、WebServer1 和 WebServer2。



▲图 9-8 配置静态端口映射

配置端口映射的步骤如下。

（1）在 CPE 上配置静态端口映射。

```
CPE>en
CPE#config t
CPE（config）#ip NAT inside source static tcp 10.0.0.5 80 131.107.0.1 80
CPE（config）#ip NAT inside source static tcp 10.0.0.6 80 131.107.0.1 81
CPE（config）#ip NAT inside source static tcp 10.0.0.4 25 131.107.0.1 25
CPE（config）#ip NAT inside source static tcp 10.0.0.4 110 131.107.0.1 110
CPE（config）#interface fastEthernet 0/1
CPE（config-if）#ip NAT inside
CPE（config-if）#ex
CPE（config）#interface Serial 0/0
CPE（config-if）#ip NAT outside
```

（2）在 Internet 的计算机 PC5 上测试端口映射，注意访问的公网地址 131.107.0.1 的不同端口，如图 9-9 和图 9-10 所示。



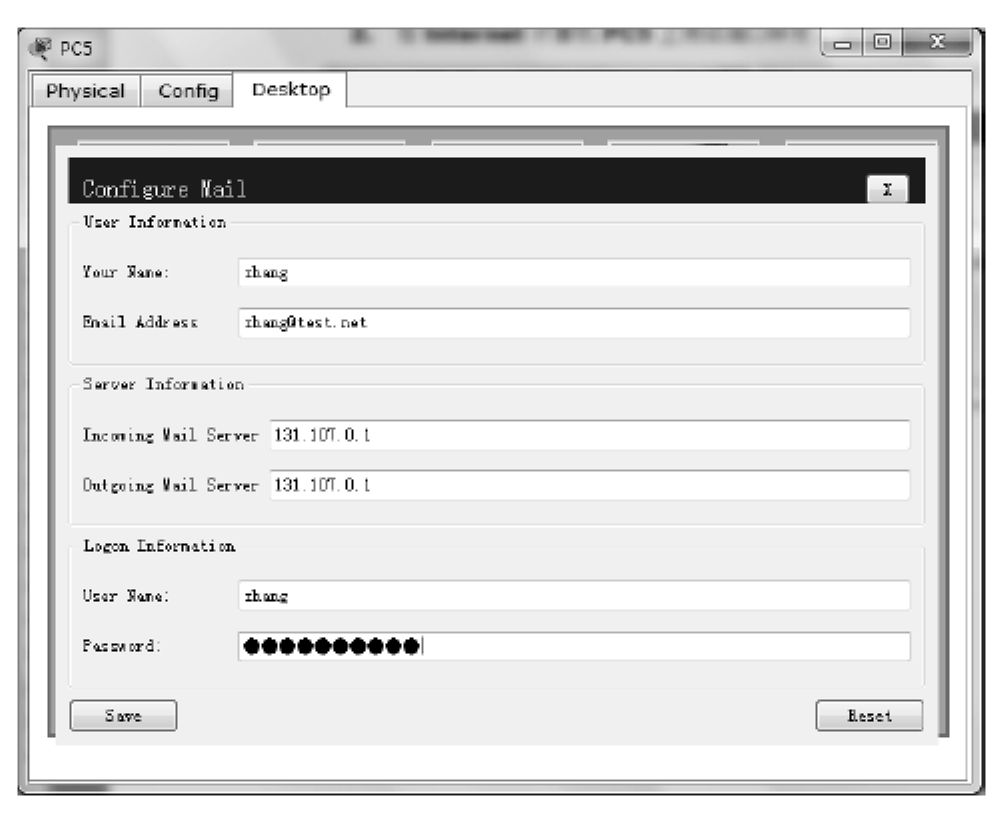


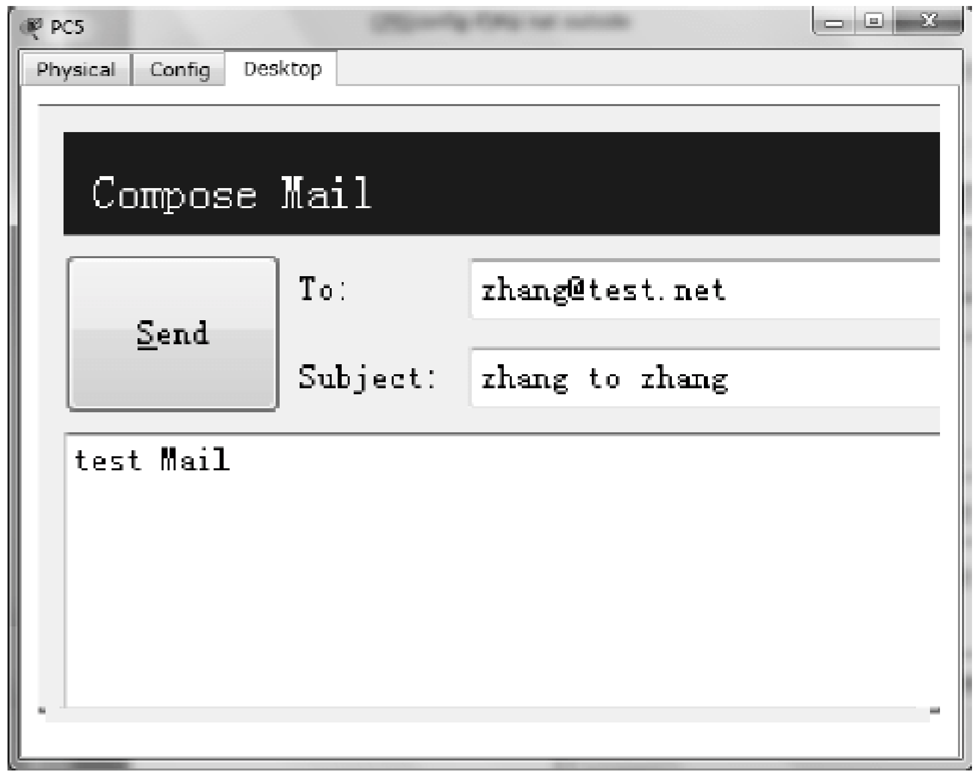
▲图 9-9　访问内网网站 1

▲图 9-10　访问内网网站 2

（3）按照图 9-11 所示，配置邮件客户端，密码为 password1!，注意收发电子邮件服务器都是 131.107.0.1，保存配置。

（4）如图 9-12 所示，给自己发一封电子邮件。





▲图 9-11　配置邮件客户端

▲图 9-12　发送电子邮件

（5）如图 9-13 所示，单击 Receive 按钮，能够收到邮件。

以上实验证明端口映射成功。



▲图 9-13　收到电子邮件

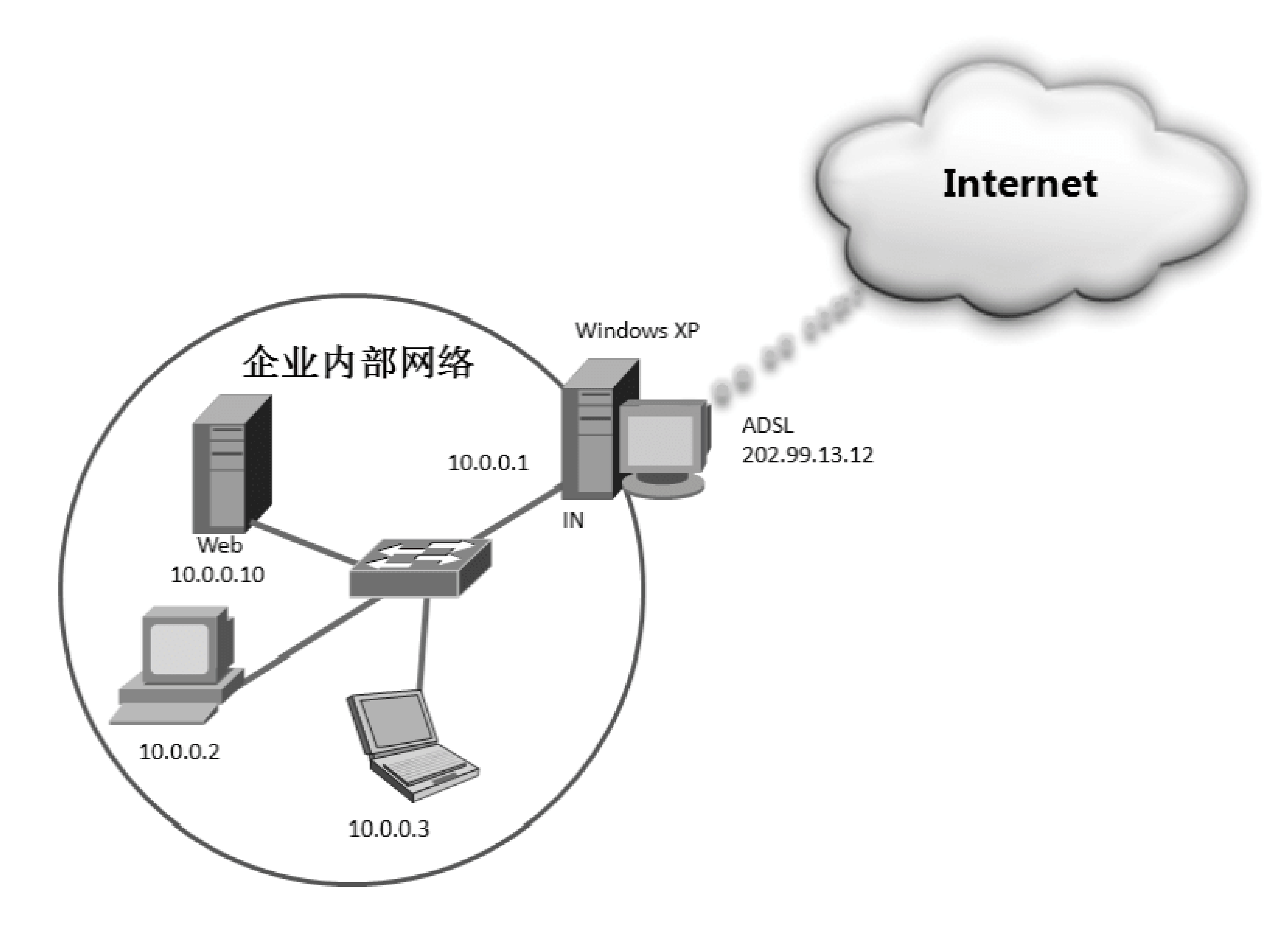
9.3 在 Windows 上实现网络地址转换和端口映射

在 Windows 中网络地址转换就是前面介绍的 PAT 的概念，特此说明。

Windows XP 或 Windows Server 2003 也能够实现 PAT 和端口映射，并且这种应用在规模较小的企业中会经常用得到。下面将为大家介绍在 Windows XP 上配置 Internet 连接共享实现的 PAT 和端口映射以及 Windows Server 2003 上实现的网络地址转换和端口映射。

9.3.1 在 Windows XP 上配置连接共享和端口映射

如图 9-14 所示，一个小的公司使用安装 Windows XP 操作系统的 ADSL 拨号访问 Internet。该主机还有一个网卡连接内网的交换机，内网的计算机需要通过 Windows XP 访问 Internet。这就需要在 Windows XP 上将 ADSL 拨号的连接共享给内网计算机，同时你也可将内网的 Web 服务器通过端口映射允许 Internet 用户访问。



▲图 9-14　配置连接共享

1. 在 Windows XP 上配置 Internet 连接共享的步骤

（1）选择“开始”→“设置”→“网络连接”命令，选中 ADSL 拨号建立的连接，右击，在弹出的快捷菜单中选择“属性”命令。

（2）如图 9-15 所示，在出现的“ADSL 属性”对话框的“高级”选项卡中选中“允许其他网络用户通过此计算机的 Internet 连接来连接”复选框。

注意	如果你的计算机只一个本地连接，不会出现“Internet 连接共享”选项组，你可以禁用一个网卡试试，如图 9-16 所示。



▲图 9-15　启用连接共享　　▲图 9-16　没有了“Internet 连接共享”选项组

（3）如图 9-17 所示，单击“确定”按钮，会出现提示对话框，提示将 LAN 连接的 IP 地址配置成 192.168.0.1。单击“是”，完成连接共享。

你再把连接内网的连接 IP 地址更改为 10.0.0.1。注意，内网的连接不设置网关。

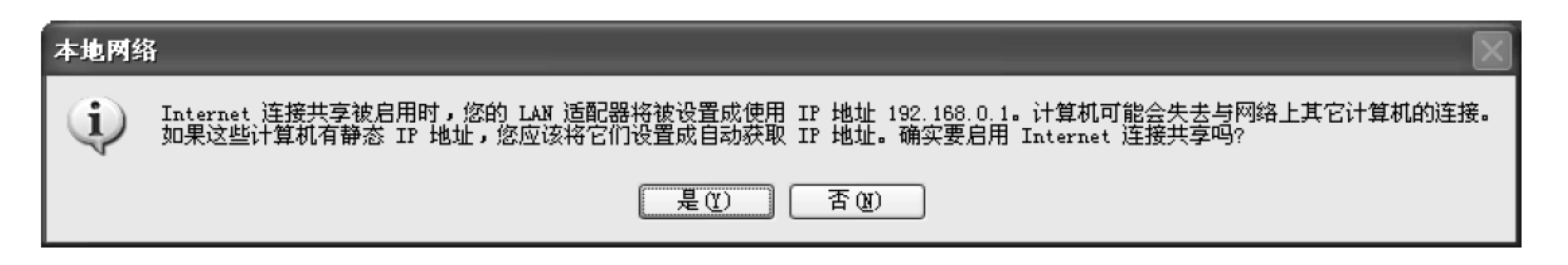
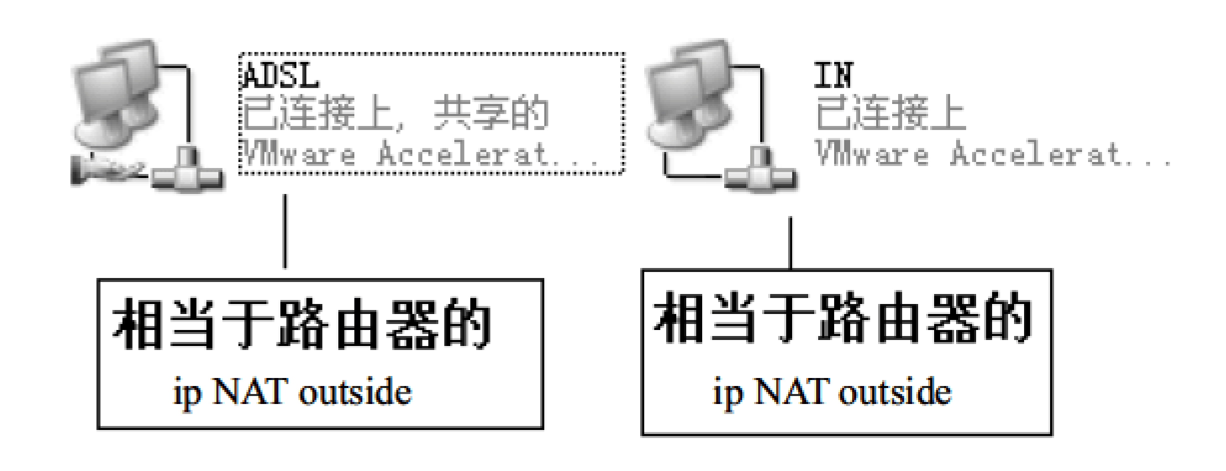


图 9-17　提示

（4）如图 9-18 所示，再看连接共享的图标，已经有了使用共享的图标标识，相当于在路由器的外网网卡上运行了 ip NAT outside 命令。



▲图 9-18　配置了连接共享的网卡

在 Windows XP 上配置 PAT 就这么简单。

2．配置端口映射的步骤

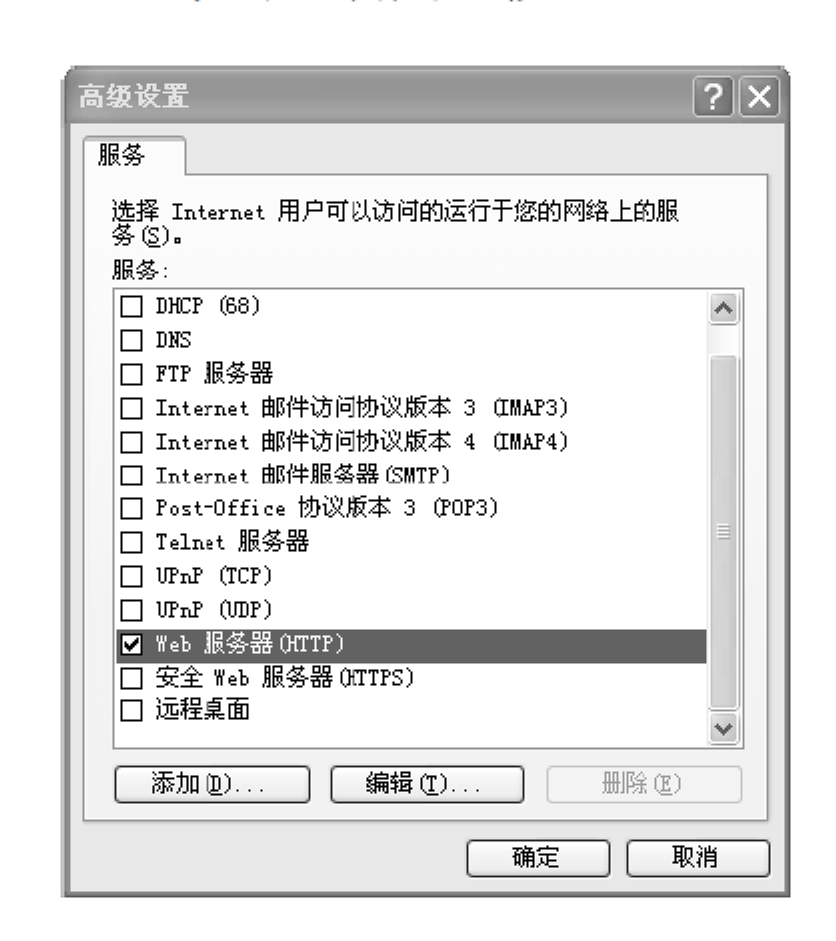
（1）如图 9-19 所示，打开“ADSL 属性”对话框，在“高级”选项卡中，单击“设置”按钮。



▲图 9-19 “ADSL 属性”对话框

（2）如图 9-20 所示，在出现的“高级设置”对话框中，选中“Web 服务器（HTTP）”复选框，单击“编辑”按钮。

（3）如图 9-21 所示，在出现的“服务设置”对话框中，输入内网 Web 服务器的 IP 地址，单击“确定”按钮。



▲图 9-20 配置 Web 服务器端口映射



▲图 9-21 指定内网 Web 服务器地址

端口映射完成。在 Windows XP 上配置端口映射也很简单。

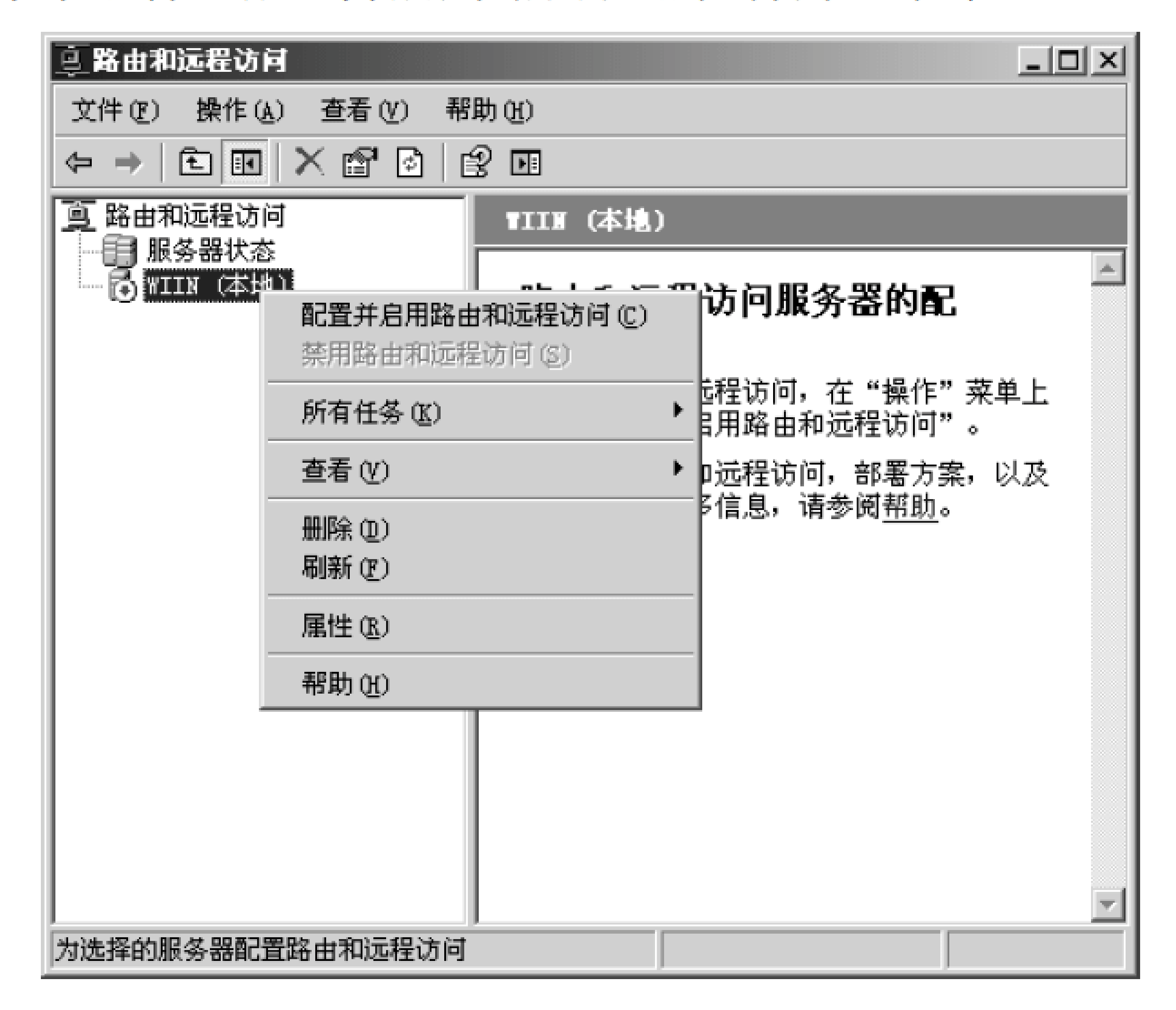
9.3.2 在 Windows Server 2003 上配置网络地址转换和端口映射

在 Windows Server 2003 上可以配置 Internet 连接共享实现 PAT 和端口映射，还可以使用路由和远程访问配置网络地址转换和端口映射实现 PAT 和端口映射。

1. 配置网络地址转换

（1）选择“开始”→“程序”→“管理工具”→“路由和远程访问”命令。

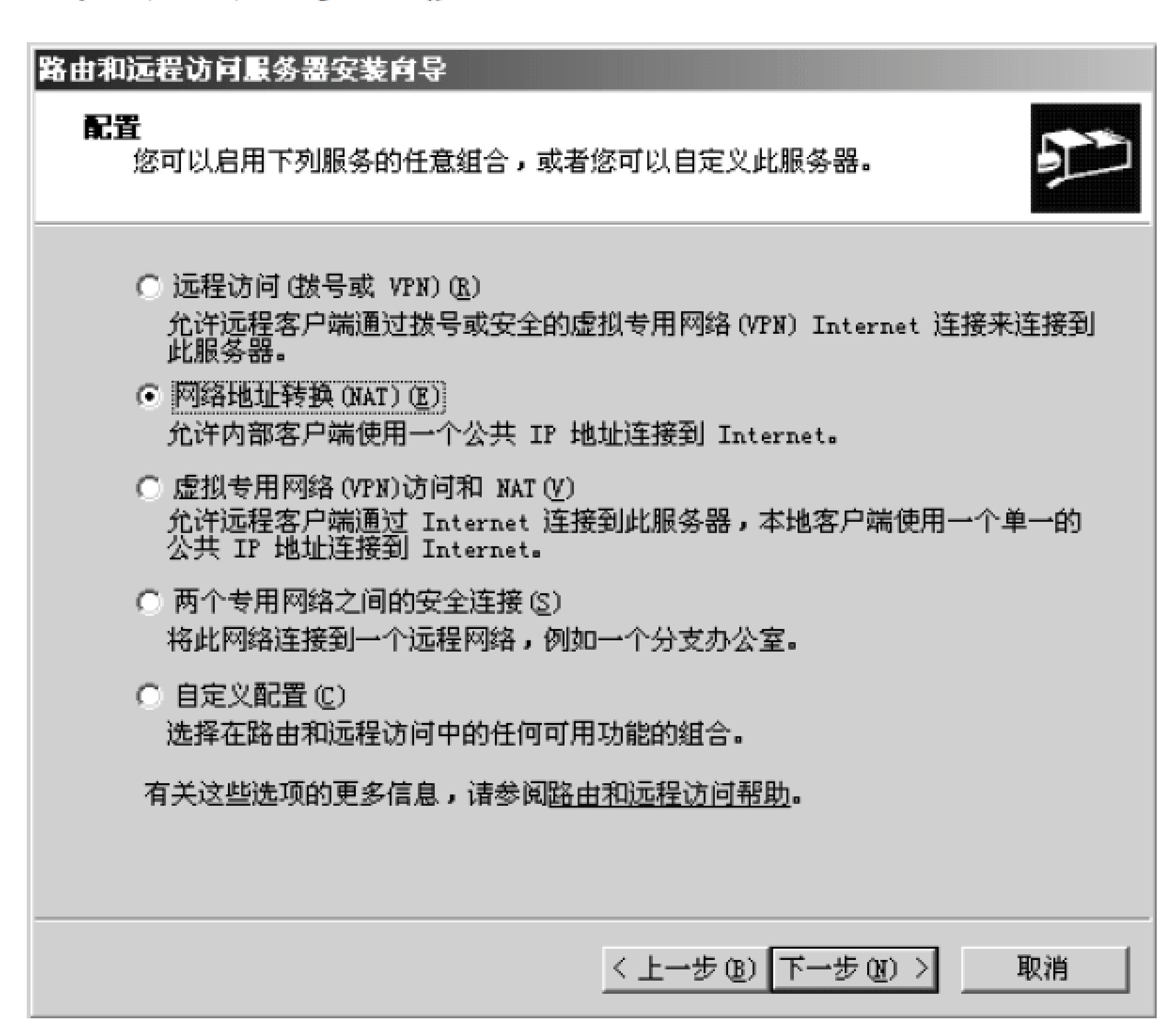
（2）如图 9-22 所示，在出现的“路由和远程访问”窗口中，右击服务器，在弹出的快捷菜单中选择“配置并启用路由和远程访问”命令。



▲图 9-22 配置并启用路由和远程访问

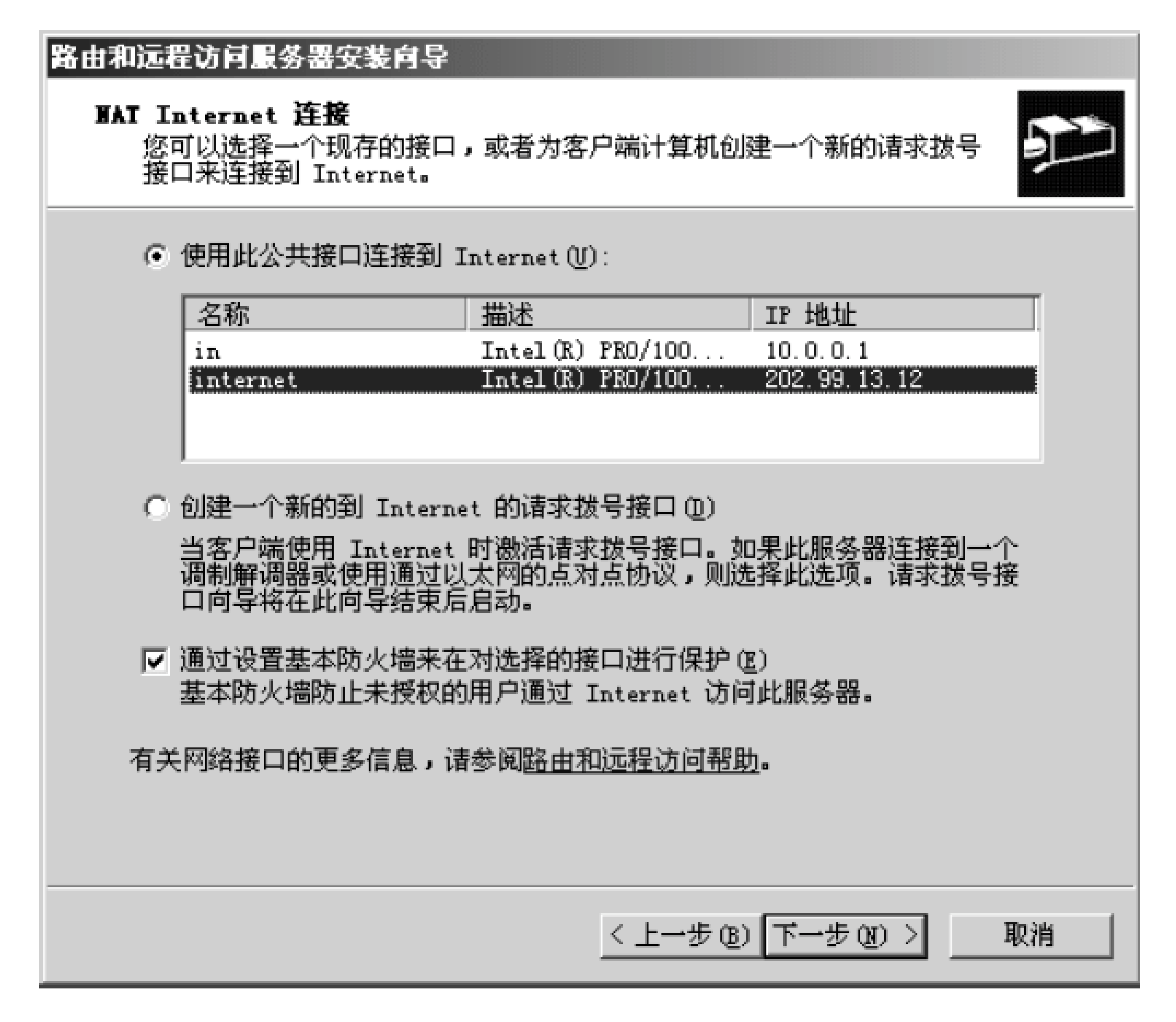
（3）在出现的“欢迎使用路由和远程访问服务器安装向导”对话框中，单击“下一步”按钮。

（4）如图 9-23 所示，在出现的“配置”设置界面中，选中“网络地址转换（NAT）”单选按钮，单击“下一步”按钮。



▲图 9-23 “配置”设置界面

（5）如图 9-24 所示，在出现的“NAT Internet 连接”设置界面中，选中“使用此公共接口连接到 Internet”单选按钮，单击“下一步”按钮。



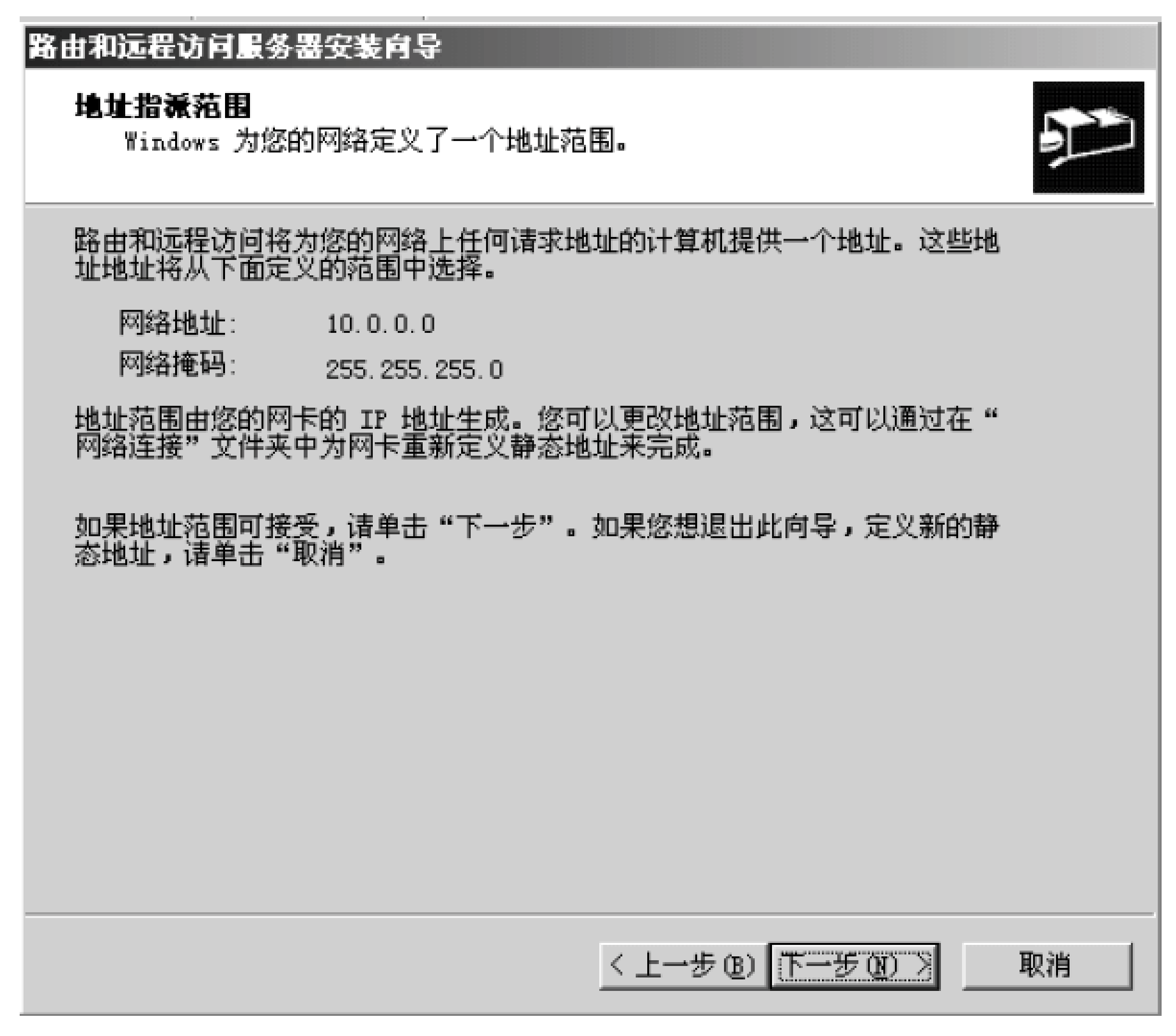
▲图 9-24 “NAT Internet 连接”设置界面

（6）如图 9-25 所示，在出现的“名称和地址转换服务”设置界面中，保持默认选项，单击“下一步”按钮。该服务器可以为内网计算机分配 IP 地址和提供域名解析服务。



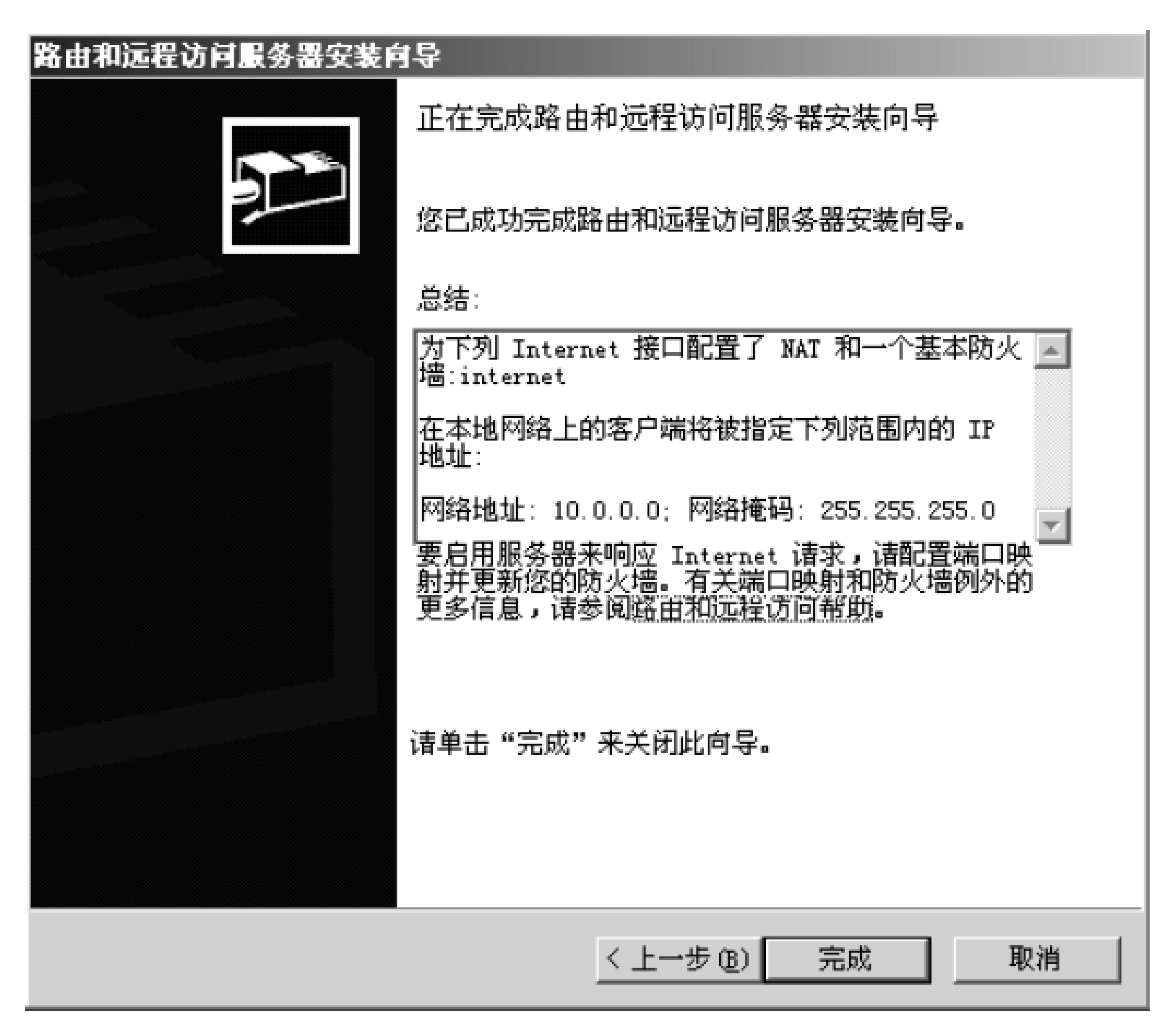
▲图 9-25 “名称和地址转换服务”设置界面

（7）如图 9-26 所示，在出现的“地址指派范围”设置界面中，单击“下一步”按钮。



▲图 9-26 “地址指派范围”设置界面

（8）如图 9-27 所示，在出现的“正在完成路由和远程访问服务器安装向导”界面中，单击“完成”按钮。



▲图 9-27 完成网络地址转换配置

2. 配置端口映射

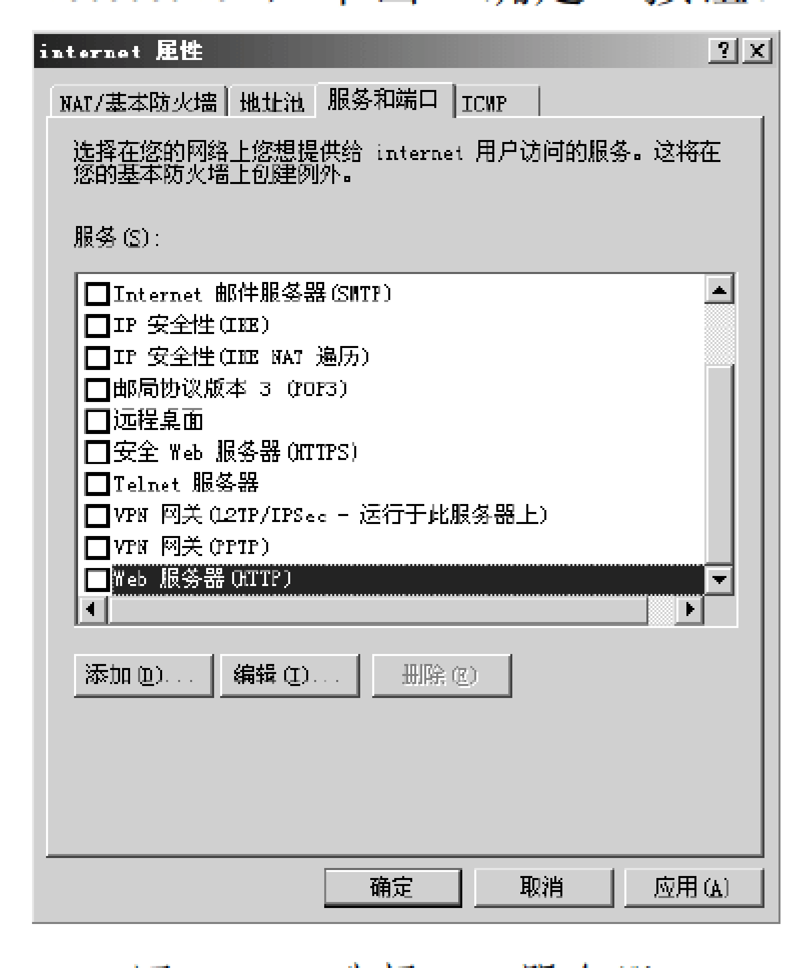
（1）如图 9-28 所示，右击 Internet 连接，在弹出的快捷菜单中选择“属性”命令。



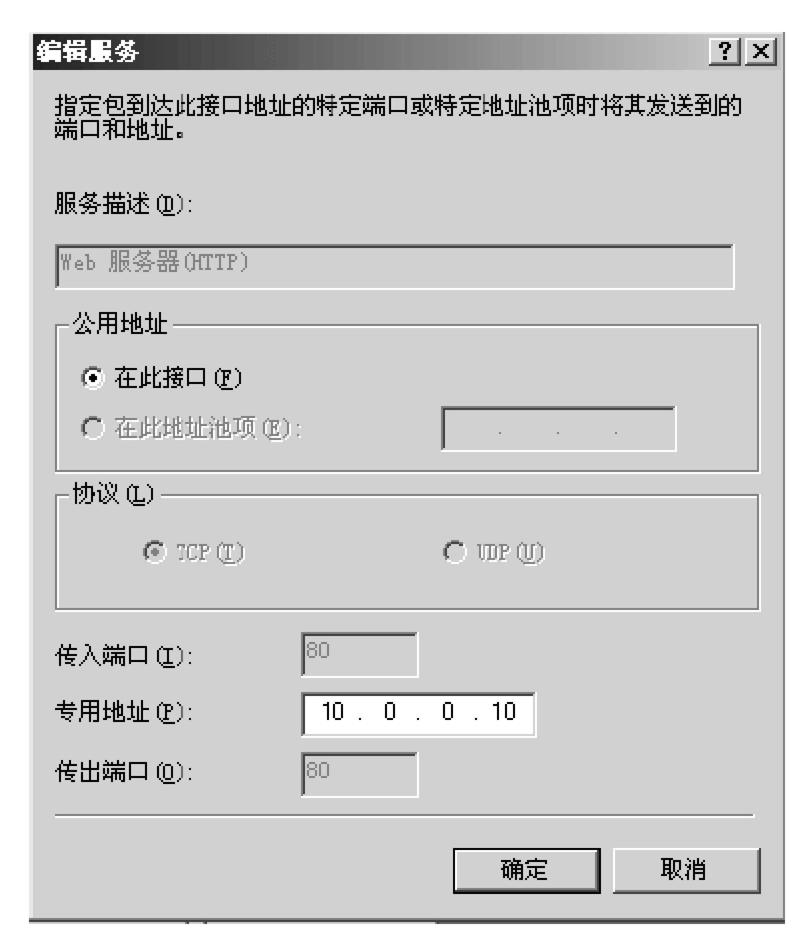
▲图 9-28 “路由和远程访问”对话框

（2）如图 9-29 所示，在出现的“Internet 属性”对话框的“服务和端口”选项卡中，选中“Web 服务器（HTTP）”复选框。

（3）如图 9-30 所示，在出现的“编辑服务”对话框的“专用地址”文本框中输入“10.0.0.10”，单击“确定”按钮。



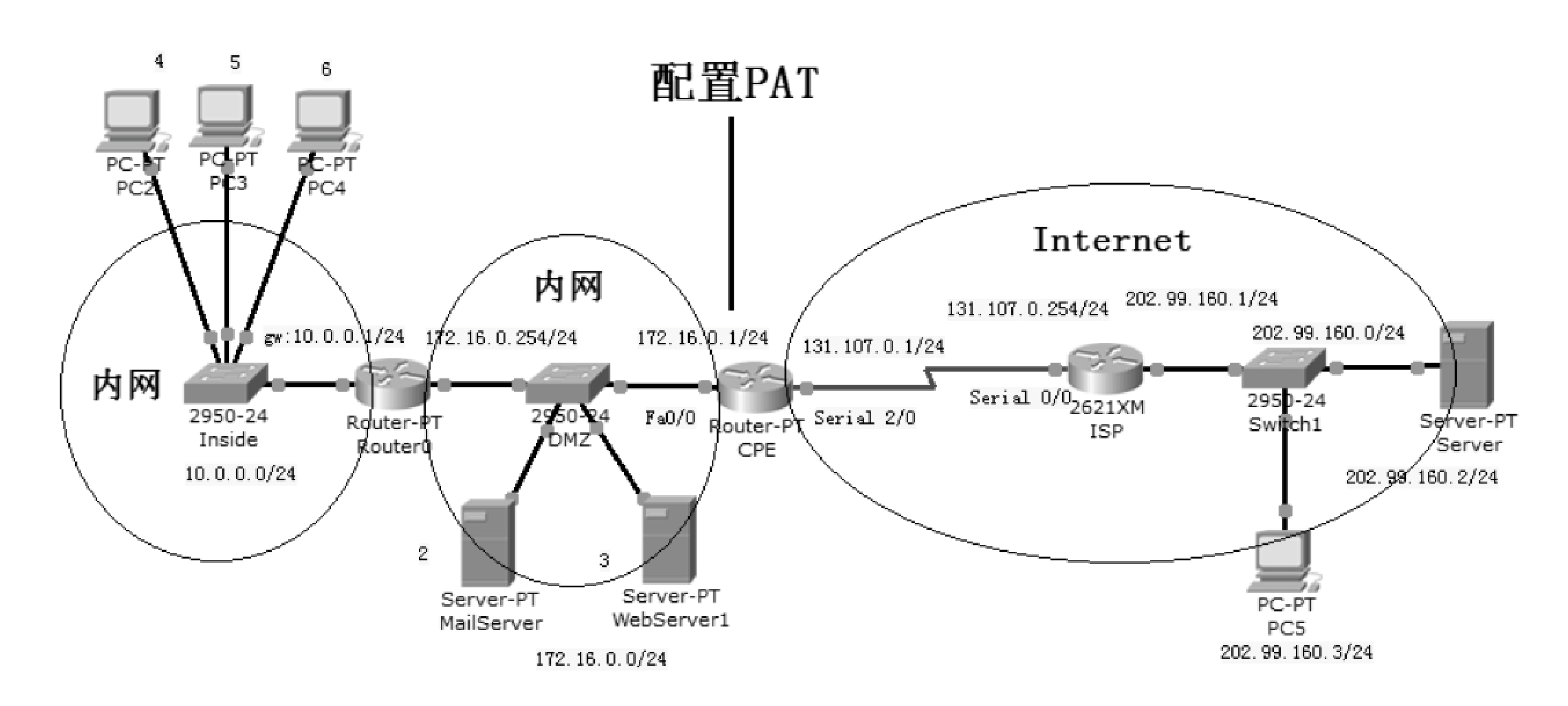
▲图 9-29 选择 Web 服务器



▲图 9-30 指定内网的 IP 地址

9.4 实验

打开随书光盘中第 9 章练习“实验 01 PAT.pkt”，网络拓扑如图 9-31 所示。你需要在 CPE 路由器上配置 PAT，允许内网的两个网段访问 Internet。



▲图 9-31　配置 PAT 实验环境

操作步骤如下。

在 CPE 上的配置：

```
CPE（config）#access-list 10 permit 10.0.0.0 0.0.0.255
CPE（config）#access-list 10 permit 172.16.0.0 0.0.0.255
CPE（config）#ip NAT pool todd 131.107.0.1 131.107.0.1 netmask 255.255.255.0
CPE（config）#ip NAT inside source list 10 pool todd overload
CPE（config）#interface Serial 2/0
CPE（config-if）#ip NAT outside
CPE（config-if）#exi
CPE（config）#interface fastEthernet 0/0
CPE（config-if）#ip NAT inside
```

注意　访问控制列表要包括内网的两个网段。

9.5　习 题

1. Internet 上路由器不进行转发的网络地址是______。

A. 101.1.32.7

B. 192.178.32.2

C. 172.16.32.1

D. 172.35.32.244

2. 北京佳城公司有一个 25 台计算机组建的局域网，打算使该网络中的计算机能够同

时访问 Internet，但是佳城公司只有 4 个可用的公网地址，如何配置才能使这 25 台计算机能够访问 Internet？________

A. Static NAT

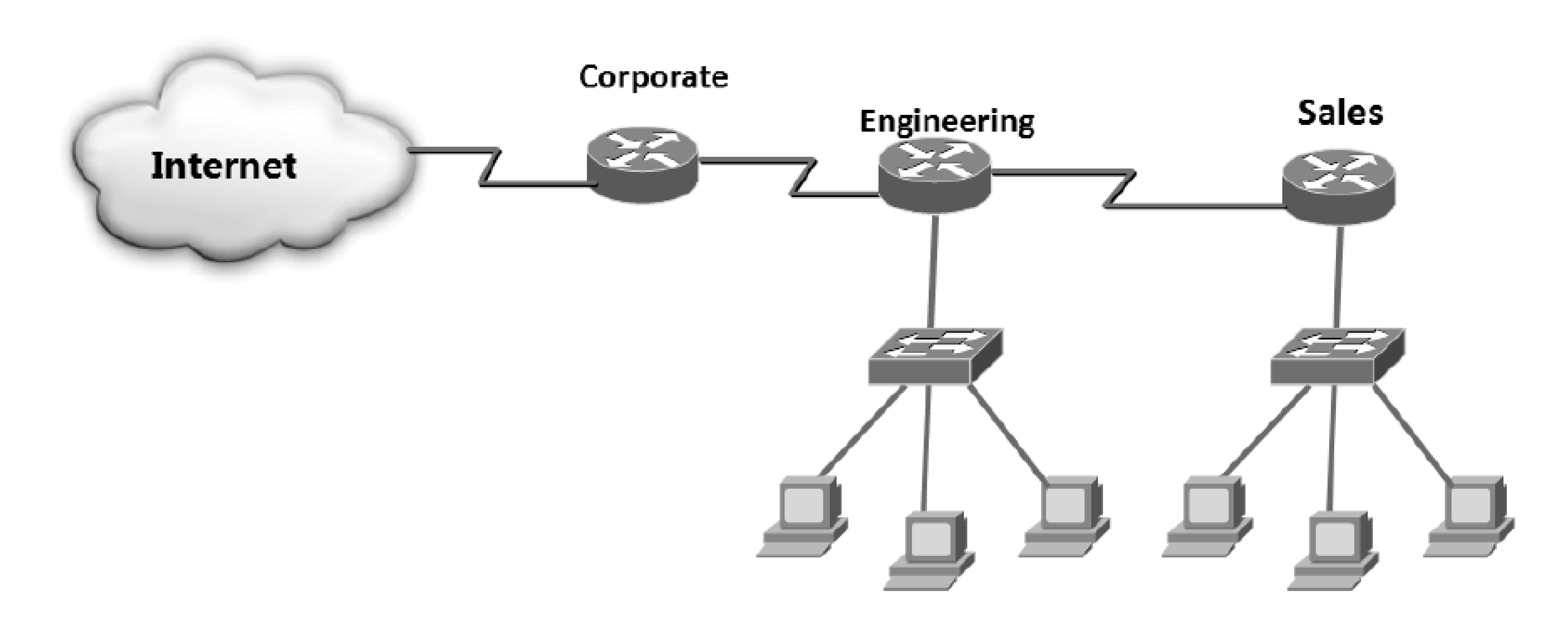
B. Global NAT

C. Dynamic NAT

D. Static NAT with ACLs

E. Dynamic NAT with overload

3. 石家庄新迈科技公司的网络拓扑如图 9-32 所示，网络管理员打算使用网络地址转换技术使内网能够访问 Internet，内网计算机使用的是私网地址，应该在______上进行 NAT 配置。



▲图 9-32　网络拓扑

A. Corporate 路由器

B. Engineering 路由器

C. Sales 路由器

D. 所有的路由器

E. 所有的路由器和交换机

4. Cisco 路由器已经使用以下命令进行了配置：

ip NAT pool NAT-test 192.168.6.10 192.168.6.20 netmask 255.255.255.0

这是________。

A. 静态 NAT

B. 动态 NAT

C. 带 overload 的动态 NAT

D. 端口地址转换 PAT

5. ________是 NAT 的缺点。（选择 3 个）

A. 导致转发延迟

B. 节省了合法的公网地址

C. 破坏了端到端的连接性

D. 增加了接入 Internet 的灵活性

E. 在使用网络地址转换的情况下某些应用程序将不能工作

F. 减少了 IP 地址重叠

6. ________命令可以看到路由器上实时的地址转换。

A. Show ip NAT translation

B. Show ip NAT statistics

C. Debug ip NAT

D. Cleare ip NAT translations

7. ________命令将会清除所有路由器上的转换活动。

A. Show ip NAT translations

B. Show ip NAT statistics

C. Debug ip NAT

D. Clear ip NAT translations *

8. ________命令将会显示 NAT 配置的汇总信息。

A. Show ip NAT translations

B. Show ip NAT statistics

C. Debug ip NAT

D. Clear ip NAT translations *

9. ________命令将会创建一个名称为 Todd 的提供 30 个公网地址的动态地址池。

A. Ip NAT pool Todd 171.16.10.65 172.16.10.94 net 255.255.255.240

B. Ip NAT pool Todd 171.16.10.65 172.16.10.94 net 255.255.255.224

C. Ip NAT pool todd 171.16.10.65 172.16.10.94 net 255.255.255.224

D. Ip NAT pool Todd 171.16.10.65 172.16.10.94 net 255.255.255.0

10. 地址转换的类型有_______。

A. Static

B. IP NAT pool

C. Dynamic

D. NAT double-translation

E. Overload

11. _______是使用网络地址转换的理由。

A. 需要连接 Internet 但是没有足够的公网地址

B. 改变了一个新的 ISP，需要重新更改内网 IP 地址

C. 不想任何主机连接 Internet

D. 有需要合并相同网段的内网

习题答案

1．C

2．E

3．A

4．B

5．A、B、D

6．C

7．A

8．D

9．B，地址池名称区分大小写

10．A、C、E

11．A、B、D

第 10 章　IPv6

本章将介绍 IPv6 比现在的 IP 有哪些方面的改进。具体介绍 IPv6 的地址体系，IPv6 下的计算机地址配置方式，IPv6 的静态路由和动态路由，支持 IPv6 的动态路由协议 RIPng、EIGRPv6 和 OSPF v3 的配置，IPv6 和 IPv4 共存技术，双协议栈技术，6 to 4 的隧道技术，ISATAP 隧道和 NAT-PT 技术。

本章主要内容：

- 为什么需要 IPv6
- IPv6 地址体系
- IPv6 下的计算机 IP 地址配置方式
- IPv6 的静态路由和动态路由
- IPv6 和 IPv4 的共存技术

10.1 为什么需要 IPv6

从 20 世纪 70 年代开始，互联网技术就以超出人们想象的速度迅猛发展。然而，随着基于 IPv4 协议的计算机网络特别是 Internet 的迅速发展，互联网在产生了巨大的经济效益和社会效益的同时也暴露出其本身固有的问题，如安全性不高、路由表过度膨胀，特别是 IPv4 地址的匮乏。随着互联网的进一步发展特别是未来电子、电器设备和移动通信设备对 IP 地址的巨大需求，IPv4 的约 42 亿个地址空间是根本无法满足要求的。有预测表明以目前 Internet 的发展速度计算，所有 IPv4 地址将在 2012 年分配完毕。这也是推动下一代互联网协议 IPv6 研究的主要动力。

10.1.1 IPv4 的不足之处

IPv4 的不足主要体现在以下几个方面。

1. 地址空间的不足

在 Internet 发展的初期，人们认为网络地址是不可能分配完的，这就导致网络地址分配时的随意性，其结果就是 IP 地址的利用率较低。由于组织的存在，IP 地址不是一个接一个地分配的，而且由于缺乏经验的地址分类的做法，造成了大量的地址浪费。

分配的过程是按时间顺序进行的，刚开始的时候一个学校可以拥有一个 A 类网络，而后来一个国家可能只能拥有一个 C 类网络。A 类网络的数目并不多，因此问题的焦点就集中在 B 类和 C 类网络地址上，A 类的网络太大，而 C 类的网络太小，因为后来的几乎所有的申请者都愿意申请一个 B 类网络，一个 B 类网络可以拥有 65534 个主机地址，而实际上根本用不了这么多的地址，由于这样的低效率的分配方法，导致 B 类地址消耗得特别快。也就导致对现有的 IP 地址的分配速率很快，造成 IP 地址即将被分配完的局面。

2. 对现有路由技术的支持不够

由于历史原因，今天的 IP 地址空间的拓扑结构都只有两层或者三层，这在路由选择上来看是非常糟糕的。各级路由器中路由表的数目过度增长，最终的结果是使路由器不堪重负，Internet 的路由选择机制因此而崩溃。

当前，Internet 发展的瓶颈已经不再是物理线路的速率，ATM 技术，百兆/千兆以太网技术的出现使得物理线路的表现有了显著的改善，现在路由器的处理速度成为阻碍 Internet 发展的主要因素。而 IPv4 天生设计上的缺陷更大大加重了路由器的负担。

首先，IPv4 的分组报头的长度是不固定的，这样不利于在路由器中直接利用硬件来实现分组中路由信息的提取、分析和选择。

其次，目前的路由选择机制仍然不够灵活，对每个分组都进行同样过程的路由选择，没有充分利用分组间的相关性。

再次，由于 IPv4 设计时未能完全遵循端到端通信的原则，加上当时物理线路的误码率比较高，使得路由器还要具备以下两个功能。

- 根据线路的 MTU 来分段和重组过大的 IP 分组。
- 逐段进行数据校验。

这同样会造成路由器处理速度降低。

3．无法提供多样的 QoS

随着 Internet 的成功和发展，商家已经将更多的关注投向了 Internet，他们意识到其中蕴含着巨大的商机，今天乃至将来，有很多的业务应用都希望在互联网上进行。在这些业务中包括对时间和带宽要求很高的实时多媒体业务，如语音、图像等；包括对安全性要求很高的电子商务业务以及发展越来越迅猛的移动 IP 业务等。这些业务对网络 QoS 的要求各不相同。但是，IPv4 在设计时没有引入 QoS 这样的概念，设计上的不足使得它很难相应地提供丰富的、灵活的 QoS 选项。

虽然人们提出了一系列的技术，如 NAT、CIDR、VLSM、RSVP 等来缓解这些问题，但这些方法都只是权宜之计，解决不了因地址不多及地址结构不合理而导致的地址短缺的根本问题。最终 IPv6 应运而生。

10.1.2　IPv6 的改进

IPv6 相对于 IPv4 来说有以下方面的改进。

1．扩展的地址空间和结构化的路由层次

IPv6 的地址长度由 IPv4 的 32 位扩展到 128 位，全局单点地址采用支持无分类域间路由的地址聚类机制，可以支持更多的地址层次和更多的结点数目，并且使得自动配置地址更加简单。

2．简化了报头格式

IPv4 报头中的一些字段被取消或是变成可选项。尽管 IPv6 的地址长度是 IPv4 的 4 倍，但是 IPv6 的基本报头只是 IPv4 报头长度的两倍。取消了对报头中可选项长度的严格限制，增加了灵活性。

3．简单的管理：即插即用

IPv6 通过实现一系列的自动发现和自动配置功能，简化网络结点的管理和维护。已实现的典型技术包括最大传输单元发现（MTU Discovery）、邻接结点发现（Neighbor Discovery）、路由器通告（Router Advertisement）、路由器请求（Router Solicitation）、结点自动配置（Auto-configuration）等。

4．安全性

在制定 IPv6 技术规范的同时，产生了 IPSec（IP Security），用于提供 IP 层的安全性。目前，IPv6 实现了认证头(Authentication Header，AH)和封装安全载荷(Encapsulated Security Payload，ESP）两种机制。前者实现数据的完整性及对 IP 包来源的认证，保证分组确实来自源地址所标记的结点；后者提供数据加密功能，实现端到端的加密。

5．QoS 能力

报头中的“标签”字段允许鉴别属于同一数据流的所有报文，因此路径上所有路由器可以鉴别一个流的所有报文，实现非默认的服务质量或实时的服务等特殊处理。

6．改进的多点寻址方案

通过在组播地址中增加“范围”字段，允许将组播的路由限定在正确的范围之内。另一个“标志”字段允许 Intranet 区分永久性的多点地址和临时性的多点地址。

7．定义了一种新的群通信地址方式：Anycast

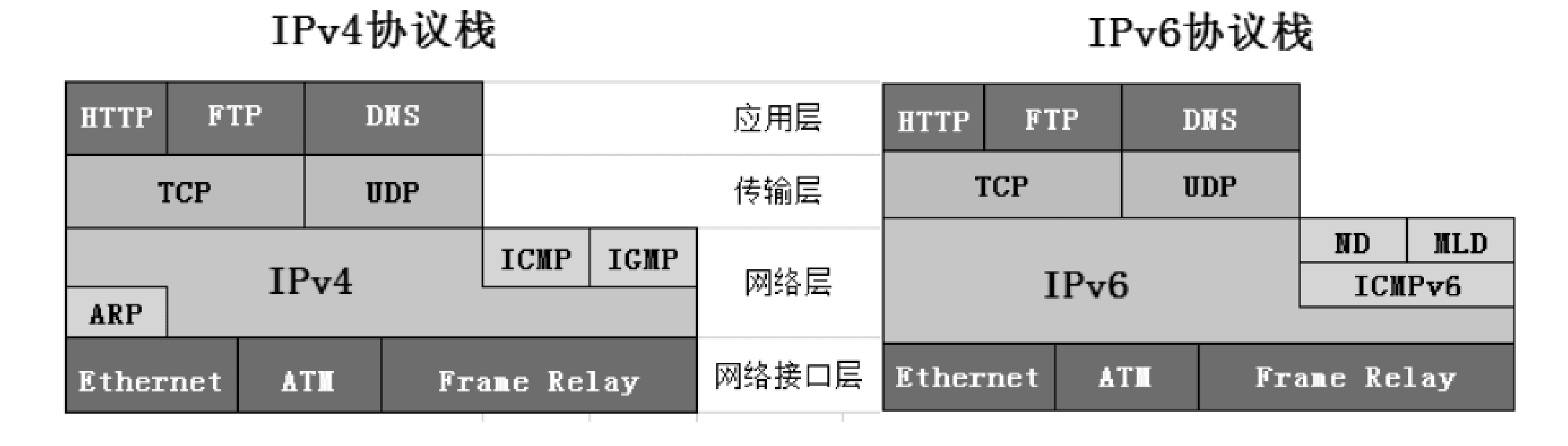
在点到多点的通信中，将报文传递到一组结点中的一个（通常是最近的一个），从而允许在源点路由中允许结点控制传递路径。

8．可移动性

IPv6 协议设计的若干技术有利于移动计算的实现，包括信宿选项头（destiNATion options header）、路由选项头（routing header）、自动配置、安全机制以及 Anycast 技术。将 QoS 技术同移动结点相结合还将强化 IPv6 对移动计算的支持。

10.1.3 IPv6 协议栈

图 10-1 所示是 IPv4 和 IPv6 协议栈的比较。



▲图 10-1　IPv6 协议栈和 IPv4 协议栈的比较

可以看到，IPv6 协议栈与 IPv4 协议栈相比较在网络层变化最大，IPv6 的网络层没有 ARP 协议和 IGMP 协议，ICMP 协议功能做了很大的扩展。ICMP 在 IPv6 定义中重新修

订。此外，IPv4 组成员协议（IGMP）的多点传送控制功能和 ARP 协议的功能也嵌入到 ICMPv6 中，分别是邻居发现 （ND） 协议和多播侦听器发现（MLD）协议。

IPv6 网络层的核心协议包括以下几种。

- IPv6：取代 IPv4，它是一个可路由协议，为数据包进行寻址、路由、分段和重组。
- Internet 控制消息协议 IPv6 版 （ICMPv6）：取代 ICMP，它报告错误和其他信息以帮助您诊断不成功的数据包传送。
- 邻居发现（ND）协议：ND 取代 ARP，它管理相邻 IPv6 结点间的交互，包括自动配置地址和将下一跃点 IPv6 地址解析为 MAC 地址。
- 多播侦听器发现（MLD）协议：MLD 取代 IGMP，它管理 IPv6 多播组成员身份。

10.1.4 ICMPv6 协议的功能

IPv6 使用的是 ICMP for IPv4 的更新版本。这一新版本叫做 ICMPv6，它执行常见的 ICMP for IPv4 功能，报告传送或转发中的错误并为疑难解答提供简单的回显服务。ICMPv6 协议还为 ND 和 MLD 消息提供消息结构。

1．邻居发现（ND）

ND 是一组 ICMPv6 消息和过程，用于确定相邻结点间的关系。ND 取代了 IPv4 中使用的 ARP、ICMP 路由器发现和 ICMP 重定向，提供了更丰富的功能。

主机可以使用 ND 完成以下任务。

- 发现相邻的路由器。
- 发现并自动配置地址和其他配置参数。

路由器可以使用 ND 完成以下任务。

- 公布它们的存在、主机地址和其他配置参数。
- 向主机提示更好的下一跃点地址来帮助数据包转发到特定目标。

结点（包括主机和路由器）可以使用 ND 完成以下任务。

- 解析 IPv6 数据包将被转发到的一个相邻结点的链路层地址（又称 MAC 地址）。
- 动态公布 MAC 地址的更改。
- 确定某个相邻结点是否仍然可以到达。

表 10-1 列出了 RFC 2461 中描述的 ND 过程并作了说明。

表 10-1 ND 过程

ND 过程	说 明
路由器发现	主机通过该过程来发现它的相邻路由器
前缀发现	主机通过该过程来发现本地子网目标的网络前缀
地址自动配置	无论是否存在地址配置服务器（例如运行动态主机配置协议 IPv6 版 （DHCPv6）的服务器），该过程都可以为接口配置 IPv6 地址

续表

ND 过程	说 明
地址解析	结点通过该过程将邻居的 IPv6 地址解析为它的 MAC 地址。IPv6 中的地址解析相当于 IPv4 中的 ARP
下一跃点确定	结点根据目标地址通过该过程来确定数据包要转发到的下一跃点 IPv6 地址。下一跃点地址可能是目标地址，也可能是某个相邻路由器的地址
邻居不可访问性检测	结点通过该过程确定邻居的 IPv6 层是否能够发送或接收数据包
重复地址检测	结点通过该过程确定它打算使用的某个地址是否已被相邻结点占用
重定向功能	该过程提示主机更好的第一跃点 IPv6 地址来帮助数据包向目标传送

2. 地址解析

IPv6 地址解析包括交换“邻居请求”和“邻居公布”消息，从而将下一跃点 IPv6 地址解析为其对应的 MAC 地址。发送主机在适当的接口上发送一条多播“邻居请求”消息。“邻居请求”消息包括发送结点的 MAC 地址。

当目标结点接收到“邻居请求”消息后，将使用“邻居请求”消息中包含的源地址和 MAC 地址的条目更新其邻居缓存（相当于 ARP 缓存）。接着，目标结点向“邻居请求”消息的发送方发送一条包含它的 MAC 地址的单播“邻居公布”消息。

接收到来自目标的“邻居公布”后，发送主机根据其中包含的 MAC 地址使用目标结点条目来更新它的邻居缓存。此时，发送主机和“邻居请求”的目标就可以发送单播 IPv6 通信量了。

3. 路由器发现

主机通过路由器发现过程尝试发现本地子网上的路由器集合。除了配置默认路由器之外，IPv6 路由器发现还配置以下设置。

- IPv6 报头中的“跃点限制”字段的默认设置。
- 用于确定结点是否应当为地址和其他配置参数使用地址配置协议（例如，动态主机配置协议 IPv6 版（DHCPv6））的设置。
- 为链路定义网络前缀列表。每个网络前缀都包含 IPv6 网络前缀及其有效的和首选的生存时间。如果指示了网络前缀，主机便使用该网络前缀来创建 IPv6 地址配置而不使用地址配置协议。网络前缀还定义了本地链路上的结点的地址范围。

IPv6 路由器发现过程如下。

- IPv6 路由器定期在子网上发送多播“路由器公布”消息，以公布它们的路由器身份信息和其他配置参数（例如地址前缀和默认跃点限制）。
- 本地子网上的 IPv6 主机接收“路由器公布”消息，并使用其内容来配置地址、默认路由器和其他配置参数。
- 一个正在启动的主机发送多播“路由器请求”消息。收到“路由器请求”消息后，本地子网上的所有路由器都向发送路由器请求的主机发送一条单播“路由器公布”消息。该主机接收“路由器公布”消息并使用其内容来配置地址、默认路由器和其

他配置参数。

4．地址自动配置

IPv6 的一个非常有用的特点是，它无需使用地址配置协议（例如，动态主机配置协议 IPv6 版（DHCPv6））就能够自动进行自我配置。默认情况下，IPv6 主机能够为每个接口配置一个在子网上使用的地址。通过使用路由器发现，主机还可以确定路由器的地址、其他地址和其他配置参数。“路由器公布”消息指示是否使用地址配置协议。

5．多播侦听器发现（MLD）

MLD 是 IGMP 版本 2（用于 IPv4）的 IPv6 版本。MLD 是路由器和节点交换的一组 ICMPv6 消息，供路由器用来为各个连接的接口发现有侦听结点的 IPv6 多播地址的集合。同 IGMPv2 一样，MLD 只能发现那些至少包含一个侦听器的多播地址，而不能发现各个多播地址的单个多播侦听器的列表。RFC 2710 中对 MLD 进行了定义。

与 IGMPv2 不同，MLD 使用 ICMPv6 消息而不是定义它自己的消息结构。

MLD 消息有三种类型。

- 多播侦听器查询：路由器使用“多播侦听器查询”消息来查询子网上是否有多播侦听器。
- 多播侦听器报告：多播侦听器使用“多播侦听器报告”消息来报告它们有兴趣接收发往特定多播地址的多播通信量，或者使用这类消息来响应“多播侦听器查询”消息。
- 多播侦听器完成：多播侦听器使用“多播侦听器完成”消息来报告它们可能是子网上最后的多播组成员。

6．路径 MTU 发现（PMTU）

它能够防止 IPv6 进行任何分段，其工作原理：连接中的源结点将发送一个数据包，它等于其本地链路 MTU 的 MTU 大小，当这个数据包穿越路径送往其目的地时，任何 MTU 比当前数据包 MTU 值小的链路，将迫使中间路由器向源结点发回一个“数据包太大”的消息。这个消息告诉源结点，那条链路的最大 MTU 值是多少，这样就允许并要求源结点发送一个新的、调整过的数据包，以便它通过网络。这个过程将持续下去，直到最终到达目的地。现在，源结点就知道新路径的 MTU 值了。当传送其他的数据包时，它们将受到保护，不会被分段。

10.2 IPv6 寻址

下面讲解 IPv6 的 IP 地址的体系结构、地址类型和一些特殊的 IPv6 地址，并且讲授在 Windows XP 上安装 IPv6 协议和配置 IPv6 地址的方法。

10.2.1 IPv6 寻址及表达式

我们已经知道，IPv6 的主要改变就是地址的长度：128 位。IPv6 地址一共有 2128 个，340.282.366.920.463.374.607.431.768.211.456 这个地址数足够地球上每人拥有上千个 IP 地址。

IPv6 使用冒号将其分割成 8 个 16 比特的数组，每个数组表示成 4 位十六进制数。一般有以下四种文本表示形式。

1. 首选的格式

把 128 比特划分成 8 段，每段为 16 比特，用十六进制表示，并使用冒号等间距分隔。例如：F00D:4598:7304:3210:FEDC:BA98:7654:3210。

2. 压缩格式

在某些 IPv6 的地址形式中，很可能地址包含了长串的“0”。为书写方便，可以允许“0”压缩，即一连串的 0 可用一对冒号来取代。例如以下地址：

```
1080:0:0:0:8:8000:200C:417A
```

可以表示为：

```
1080::8:8000:200C:417A
```

但要注意，为了避免出现地址表示的不清晰，一对冒号（::）在一个地址中只能出现一次。

3. 内嵌 IPv4 的 IPv6 地址

当涉及 IPv4 和 IPv6 的混合环境时，有时使用地址表示形式 x:x:x:x:x:x:d.d.d.d，这里 6 个“x”分别代表地址中的用十六进制表示的一位数，4 个“d”分别代表地址中的 8 比特，用十进制表示。例如：

```
0:0:0:0:0:0:218.129.100.10
```

或者以压缩形式表示：

```
::218.129.100.10
```

4.“地址/前缀长度”表示法

表示形式是：IPv6 地址/前缀长度，其中“前缀长度”是一个十进制数，表示该地址的前多少位是地址前缀。例如：F00D:4598:7304:3210:FEDC:BA98:7654:3210，其地址前缀是 64 位，就可以表示为：F00D:4598:7304:3210:FEDC:BA98:7654:3210/64。

当使用 Web 浏览器向一台 IPv6 设备发起 HTTP 连接时，必须将 IPv6 地址输入浏览器，而且要用方括号将 IPv6 地址括起来。为什么呢？这是因为浏览器在指定端口号时，已经使用了一个冒号。因此，如果你不用方括号将 IPv6 地址括起来，浏览器将无法识别出信息。

下面是这种情况的一个例子：

```
http://[2001:0db8:3c4d:0012:0000:0000:1234:56ab]/default.html
```

显然，如果可以的话，你肯定愿意使用网站的域名来访问 Web 站点，比如 http://www.edu2act.org，在 IPv6 的网络中 DNS 变得尤为重要。

10.2.2 IPv6 的地址类型

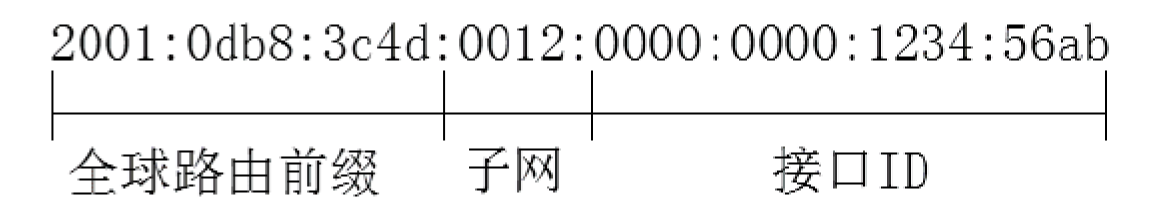
IPv6 地址是独立接口的标识符，所有的 IPv6 地址都被分配到接口，而非结点。RFE 2373 中定义了三种 IPv6 地址类型：单播地址（Unicast）、多播地址（Multicast）和任播地址（Anycast）。

1. 单播地址（Unicast）

单播地址是点对点通信时使用的地址。此地址仅标识一个接口，网络负责把对单播地址发送的数据包送到该接口上。

单播地址有全球单播地址（Global Unicast Address）、未指定地址（Unspecified Address）、环回地址（Loopback Address）等几种形式。

一般的，全球单播地址的格式如图 10-2 所示。



▲图 10-2　单播地址结构

IPv6 全局单播地址的分配方式如下：顶级地址聚集机构 TLA（即大的 ISP 或地址管理机构）获得大块地址，负责给次级地址聚集机构 NLA（中小规模 ISP）分配地址，NLA 给站点级地址聚集机构 SLA（子网）和网络用户分配地址。

全球路由前缀（global routing prefix）：典型的分层结构，根据 ISP 来组织，用来分配给站点（Site），站点是子网/链路的集合。

- 子网 ID（SubnetID）：站点内子网的标识符。由站点的管理员分层地构建。
- 接口 ID（InterfaceID）：用来标识链路上的接口。在同一子网内是唯一的。

2. 多播地址

多播地址标识一组接口（一般属于不同结点）。当数据包的目的地址是多播地址时，网络尽量将其发送到该组的所有接口上。信源利用多播功能只需生成一次报文即可将其分发给多个接收者。多播地址以 11111111 即 ff 开头。

3. 任播地址

任播地址标识一组接口，它与多播地址的区别在于发送数据包的方法。向任播地址发送的数据包并未被分发给组内的所有成员，而是发往该地址标识的“最近的”那个接口。

任播地址从单播地址空间中分配，使用单播地址的任何格式。因而，从语法上，任播地址与单播地址没有区别。当一个单播地址被分配给多于一个的接口时，就将其转化为任播地址。被分配具有任播地址的结点必须得到明确的配置，从而知道它是一个任播地址。

4．链路本地地址

IPv6 中有种地址类型叫做链路本地（link local）地址，该地址用于在同一网中的 IPv6 计算机之间进行通信。自动配置，邻居发现，没有路由器的链路上的结点都使用这类地址。任意需要将包发往单一链路上的设备和不希望包发往链路范围外的协议都可以使用链路本地地址。当你配置一个单播 IPv6 地址的时候，接口上会自动配置一个链路本地地址。链路本地地址和可路由的 IPv6 地址共存。

10.2.3　IPv6 中特殊的地址

在 IPv6 中是否会有特殊的、保留的地址，因为在 IPv4 中就有这样的地址。是的，在 IPv6 中也有很多这样的地址。

下面将列出一些地址和地址范围，大家一定要记住它们，因为肯定能用到。它们都很特殊，或者是为特定使用目的而保留的，但与 IPv4 不同的是，IPv6 的地址空间特别巨大，因此，保留一些地址确实无关紧要。

- 0:0:0:0:0:0:0:0：等于::。这是 IPv4 中 0.0.0.0 的等价物，当正在使用有状态的地址配置时，典型情况下是主机的源地址。
- 0:0:0:0:0:0:0:1：等于::1。这是 IPv4 中 127.0.0.1 的等价物。
- 0:0:0:0:0:0:192.168.100.1：这是在 IPv6/IPv4 混合网络环境中 IPv4 地址的表示式。
- 2000::/3：全球单播地址范围。写成二进制 0010 0000 0000 0000::/3，只要前三位是 001 就是全球单播地址，写成十六进制即 2xxx::/64 和 3xxx::/64 打头的都是全球单播地址。
- FE80::/10：链路本地单播地址范围。
- FF00::/8：组播地址范围。
- 3FFF:FFFF::/32：为示例和文档保留的地址。
- 2001:0DB8::/32：也是为示例和文档保留的地址。
- 2002::/16：用于 IPv6 到 IPv4 的转换系统，这种结构允许 IPv6 包通过 IPv4 网络进行传输，而无需显式地配置隧道。

10.2.4　IPv6 计算机地址配置方法

IPv6 协议的一个突出特点是支持网络结点地址自动配置，极大地简化了网络管理者的工作。下面将演示一台设备自动地为它自己配置地址的能力，这就是“无状态自动配置”；另一种自动配置类型，称为“有状态自动配置”。一定要牢记，有状态自动配置与 IPv4 中使用的 DHCP 服务器配置十分相像。

1. 无状态自动配置

自动配置是一种令人难以置信的、有用的解决方案，因为它允许网络中的设备用链路本地单播地址自动进行地址配置。这个过程在开始时从路由器那里学习前缀信息，然后将设备自己的接口地址作为接口 ID 附加上去。但它从哪里获得接口 ID 呢？大家知道，以太网中的每台设备都有一个物理 MAC 地址，这个 MAC 地址就用来作为接口 ID。可是 IPv6 地址中的接口 ID 是 64 位的，而 MAC 地址仅为 48 位，因此，需要另外再加上 16 位。这 16 位从哪里来呢？是在 MAC 地址的中间填充 FFFE。

例如，我们假定某台设备的 MAC 地址如下：

```
0060.d673.1987
```

在填充之后，就变为 0260.d6FF.FE73.1987。

那么，地址开头的 2 是从哪里来的呢？大家要知道，如果地址是本地唯一的或全球唯一的，那么填充过程的部分（称为改进的 eui-64 格式）会将一位改为特定的数字，被改动的这一位是二进制 MAC 地址中的第 7 位。这一位的值为 1，意味着是全球唯一的；这一位的值为 0，意味着是本地唯一的。看看例子，你能说出这个地址是全球唯一的还是本地唯一的么？对了，是全球唯一的。如果是 0060.d6FF.FE73.1987，这意味着是本地唯一的。

示例：安装 IPv6 并查看本地链路地址

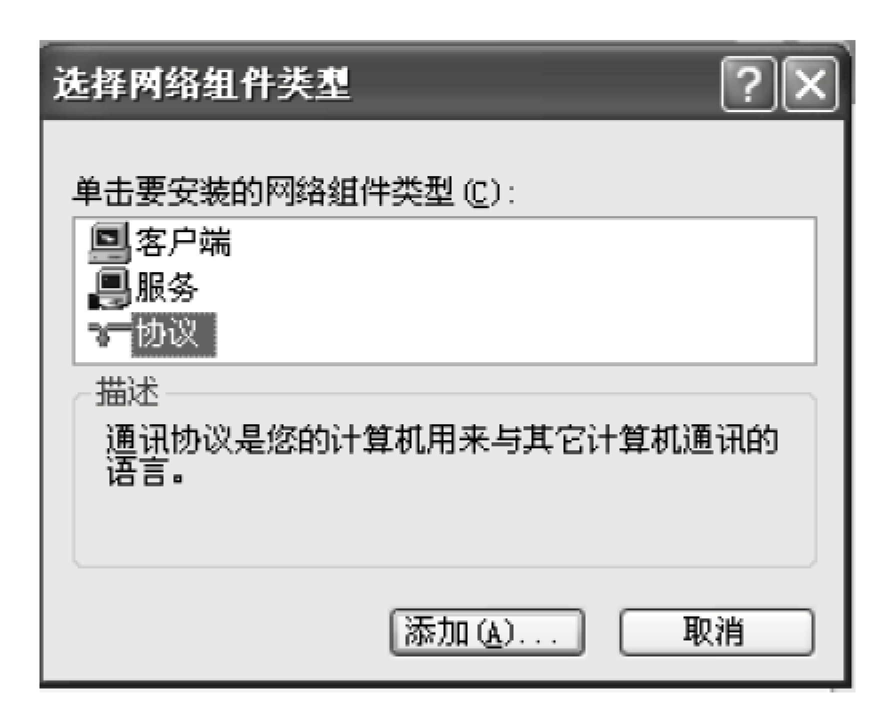
Windows Server 2003、Windows 7、Windows Server 2008 默认已经启用了 IPv6。默认 Windows XP 没有启用 IPv6 协议，你需要安装 IPv6。

（1）如图 10-3 所示，打开“本地连接 属性”对话框，在“常规”选项卡中，单击“安装”按钮。



▲图 10-3 “本地连接 属性”对话框

（2）如图 10-4 所示，在出现的“选择网络组件类型”对话框中，选中“协议”选项，单击“添加”按钮。



▲图 10-4 “选择网络组件类型”对话框

（3）如图 10-5 所示，在出现的“选择网络协议”对话框中，选择“Microsoft TCP/IP 版本 6”选项，单击“确定”按钮。



▲图 10-5 选择 IPv6

（4）如图 10-6 所示，添加了 IPv6 协议绑定到本地连接。



▲图 10-6 添加了 IPv6 协议

（5）如图 10-7 所示，在命令提示符下，输入 ipconfig 能够看到 IPv6 的本地链路地址。

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . : han-a08e3360c71
        Primary Dns Suffix    :
        Node Type . . . . . . : Unknown
        IP Routing Enabled. . : No
        WINS Proxy Enabled. . : No

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . : 00-0C-29-C5-1F-77   MAC地址
        Dhcp Enabled. . . . . : No
        IP Address. . . . . . : 10.0.1.122
        Subnet Mask . . . . . : 255.255.255.0
        IP Address. . . . . . : fe80::20c:29ff:fec5:1f77%5   本地链路地址
        Default Gateway . . . : 10.0.1.1
        DNS Servers . . . . . : 202.99.168.8
                                fec0:0:0:ffff::1%1
                                fec0:0:0:ffff::2%1
                                fec0:0:0:ffff::3%1
```

▲图 10-7　IPv6 的本地链路地址

（6）配置 Dynamips 路由器，启用 IPv6 转发，和计算机连接的网络接口 fastEthernet 1/0 的 IPv6 地址为 2001:3::1/64。

```
RA（config）#ipv6 unicast-routing                    --在路由器上启用 IPv6 转发
RA（config）#interface fastEhernet 1/0
RA（config-if）#ipv6 address 2001:3::1/64             --指定 IPv6 地址
```

提示

你也可以使用以下方式配置 IPv6 地址。

RA（config-if）#ipv6 address 2001:3::/64 eui-64

可以指定整个 128 位的全球 IPv6 地址，或者使用 eui-64 选项。记住，eui-64 格式允许设备使用其 MAC 地址并对它进行填充，以得到接口 ID。

说明

记住，如果仅有链路本地地址，将只能与本地子网上的主机通信。

要将路由器配置为仅使用链路本地地址，可使用 IPv6 enable 接口配置命令:

RA（config-if）#ipv6 enable

（7）如图 10-8 所示，查看无状态配置自动配置的 IPv6 地址和本地链路地址。本地链路地址用于本网段通信。

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . . . . . : han-a08e3360c71
    Primary Dns Suffix  . . . . :
    Node Type . . . . . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . : VMware Accelerated AMD PCNet Adapter

   Physical Address. . . . . . : 00-0C-29-C5-1F-77
   Dhcp Enabled. . . . . . . . : No
   IP Address. . . . . . . . . : 10.0.1.122
   Subnet Mask . . . . . . . . : 255.255.255.0
   IP Address. . . . . . . . . : 2001:3::8be:8bbb:b832:fdf9
   IP Address. . . . . . . . . : 2001:3::20c:29ff:fec5:1f77   无状态地址配置
   IP Address. . . . . . . . . : fe80::20c:29ff:fec5:1f77%5   本地链路地址
   Default Gateway . . . . . . : 10.0.1.1
                                 fe80::ce00:5ff:fec8:0%5   网关是路由器的本地链路地址
```

▲图 10-8 无状态地址配置的 IPv6 地址

2. 有状态自动配置

大家可能会感到吃惊，但确实有一些其他的选项是 DHCP 仍然提供而自动配置却不能提供的。无状态自动配置中，绝对没有提到 DNS 服务器、域名服务，或者其他许多选项，这些都是 DHCP 在 IPv4 自动配置中一直提供的。这就是为什么在大多数情况下，我们可能仍然要在 IPv6 中使用 DHCP 的原因。

IPv4 中，在引导期间，客户端发送一个 DHCP 发现消息，以查找服务器，得到它所需要的信息。但要记住，在 IPv6 中，首先发生 RS 和 RA 过程。如果网络中有一台 DHCPv6 服务器，返回到客户端的 RA 将告诉它 DHCP 服务器是否可用。如果没有找到路由器，客户端将发送 DHCP 征求消息。征求消息实际上就是组播消息，源地址为 ff02::1:2，意味着所有的 DHCP 代理，包括服务器和中继器都响应该征求信息。

Windows Server 2008 的 DHCP 服务器支持 IPv6。

3. 指定静态 IPv6 地址

对于服务器来说，为了客户端访问方便，最好指定固定的 IPv6 地址，以便客户端能够较容易地找到。Windows XP 和 Windows Server 2003 没有提供图形界面配置 IPv6 的地址、网关以及 DNS 等。以下命令是在 Windows XP 上运行的，可以指定本地连接的 IPv6 地址、网关和 DNS 服务器。

```
    C:\Documents and Settings\Administrator>netsh interface ipv6 add address
"本地连接" 2001:3::2
    C:\Documents and Settings\Administrator>netsh interface ipv6 add route ::/0
"本地连接"  2001:3::1
    C:\Documents and Settings\Administrator>netsh interface ipv6 add dns "本
地连接"
     2001:3::100
```

查看 IPv6 的配置，如图 10-9 所示。

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : han-a08e3360c71
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 本地连接:

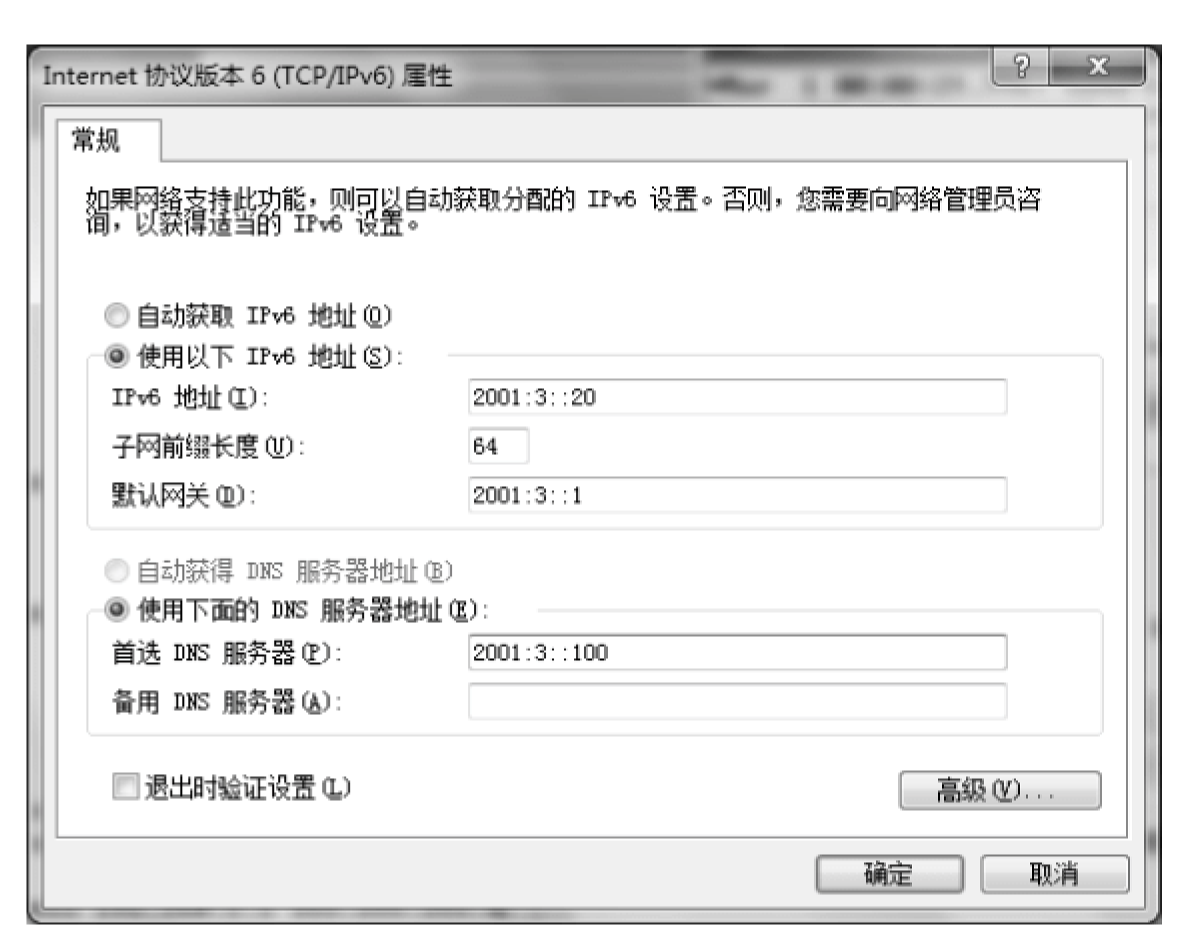
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . . . . . . . : 00-0C-29-C5-1F-77
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.0.1.122
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:3::2    指定的静态IPv6地址
        IP Address. . . . . . . . . . . . : fe80::20c:29ff:fec5:1f77%5
        Default Gateway . . . . . . . . . : 10.0.1.1
                                            2001:3::1
        DNS Servers . . . . . . . . . . . : 202.99.168.8
                                            2001:3::100
```

▲图 10-9　指定的静态 IPv6 地址

将以上命令中的 add 换成 delete，就可以删除 IPv6 地址、DNS 和网关。

如图 10-10 所示，Windows Server 2008、Windows 7 和 Vista 操作系统中的 IPv6 可以这样指定 IPv6 的配置。



▲图 10-10　指定静态 IPv6 地址

10.3 配置 IPv6 路由

在网络规模不大的情况下，IPv6 环境也可以使用静态路由。配置 IPv6 的静态路由和配置 IPv4 的静态路由一样。路由器要知道到达所有网络的路由。

为了在 IPv6 网络中使用，前面讨论过的大多数路由协议已经升级了。我们讨论过的许多功能和配置，将以几乎一样的方式在这里继续得到应用。大家知道，在 IPv6 中取消了广播地址，因此，完全使用广播流量的任何协议都不会再用了，这是一件好事情，因为它们消耗了大量的带宽。

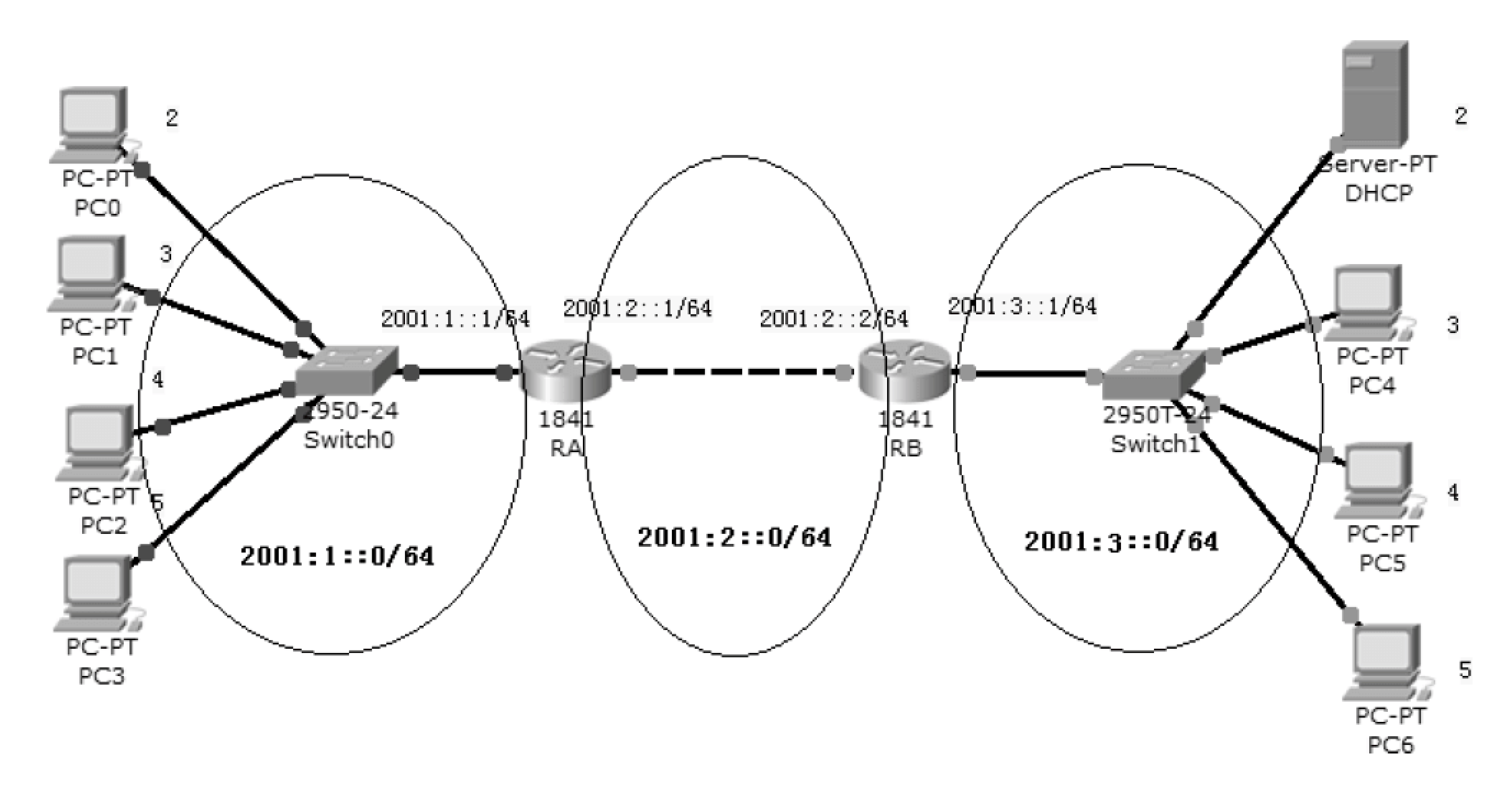
在 IPv6 中仍然使用的路由协议都有了新的名字，并做了翻新。

首先是 RIPng（下一代 RIP）。如果你已经在 IT 行业工作了一段时间，就会知道 RIP 在小型网络中工作得很好。正是因为这一点，使得 RIP 一直沿用了下来，还将应用在 IPv6 网络中。我们还会使用 EIGRPv6，因为它已经有了与协议有关的模块，我们所要做的只是向其中添加 IPv6 协议即可。剩下的路由协议就是 OSPFv3 了，它是真正的第 3 版，因为 IPv4 网络中的 OSPF 实际上是第 2 版，因此，当它升级到 IPv6 时，就变成了第 3 版。

以下将会演示配置 IPv6 的静态路由，配置支持 IPv6 的动态路由协议 RIPng、EIGRPv6 和 OSPFv3。

10.3.1 配置 IPv6 静态路由

打开随书光盘中第 10 章练习“01 IPv6 静态路由.pkt”，网络拓扑如图 10-11 所示。网络中包括 3 个 IPv6 网段。网络中的路由器和计算机已经按照图示配置好了 IPv6 地址。你需要在 RA 和 RB 路由器上添加静态路由，使这 3 个网段的计算机能使用 IPv6 通信。



▲图 10-11　IPv6 静态路由实验环境

配置 IPv6 静态路由的步骤如下。

（1）在 RA 上查看 IPv6 的路由，没有到达 2001:3::0/64 网段的路由。

```
RA#show ipv6 route
C   2001:1::/64 [0/0]
     via ::， fastEthernet0/0
```

```
L   2001:1::1/128 [0/0]
     via ::,  fastEthernet0/0
C   2001:2::/64 [0/0]
     via ::,  fastEthernet0/1
L   2001:2::1/128 [0/0]
     via ::,  fastEthernet0/1
L   FF00::/8 [0/0]
     via ::,  Null0
```

（2）在 RA 上添加到达 2001:3::0/64 网段的静态路由。

```
RA#config t
RA（config）#ipv6 route 2001:3::/64 2001:2::2
```

（3）在 RB 上添加到 2001:1::0/64 网段的静态路由。

```
RB#config t
RB（config）#ipv6 route 2001:1::/64 2001:2::1
```

（4）在 RA 上查看路由表，显示添加的静态路由。

（5）使用 PC0 ping DHCP 计算机的 IPv6 地址，能通。

```
PC>ping 2001:3::2
```

10.3.2 配置 RIPng 支持 IPv6

RIPng 的主要特性与 RIPv2 是一样的。它仍然是距离矢量协议，最大跳数为 15，使用水平分割、毒性逆转和其他的环路避免机制，但它现在使用 UDP 端口 521。

RIPng 仍然使用组播来发送其更新信息，但在 IPv6 中，它使用 FF02::9 为传输地址。在 RIPv2 中，该组播地址是 224.0.0.9，因此，在新的 IPv6 组播范围中，地址的最后仍然有一个 9。事实上，大多数路由协议都像这样，保留了一部分 IPv4 的特征。

当然，新版本肯定与旧版本有不同之处，否则它就不是新版本了。我们知道，路由器在其路由表中，为每个目的网络保留了其邻居路由器的下一跳地址。对于 RIPng，其不同之处在于，路由器使用链路本地地址而不是全球地址来跟踪下一跳地址。

在 RIPng 中，最大的改变是，需要从接口配置模式配置或启用网络中的通告，而不是在路由器配置模式下使用 network 命令来通告（所有的 IPv6 路由协议都如此）。因此，在 RIPng 中，在接口上直接启用它而不是进入路由器配置模式并启动 RIPng 进程，那么将启动一个新的 RIPng 进程，它看起来是这样的：

输入以下命令，在路由器上启用 RIPng。

```
Router1（config）#ipv6 router rip 1
```

在这条命令中，1 是一种标记，用来识别正在运行的 RIPng 进程，可以是数字和字符串。

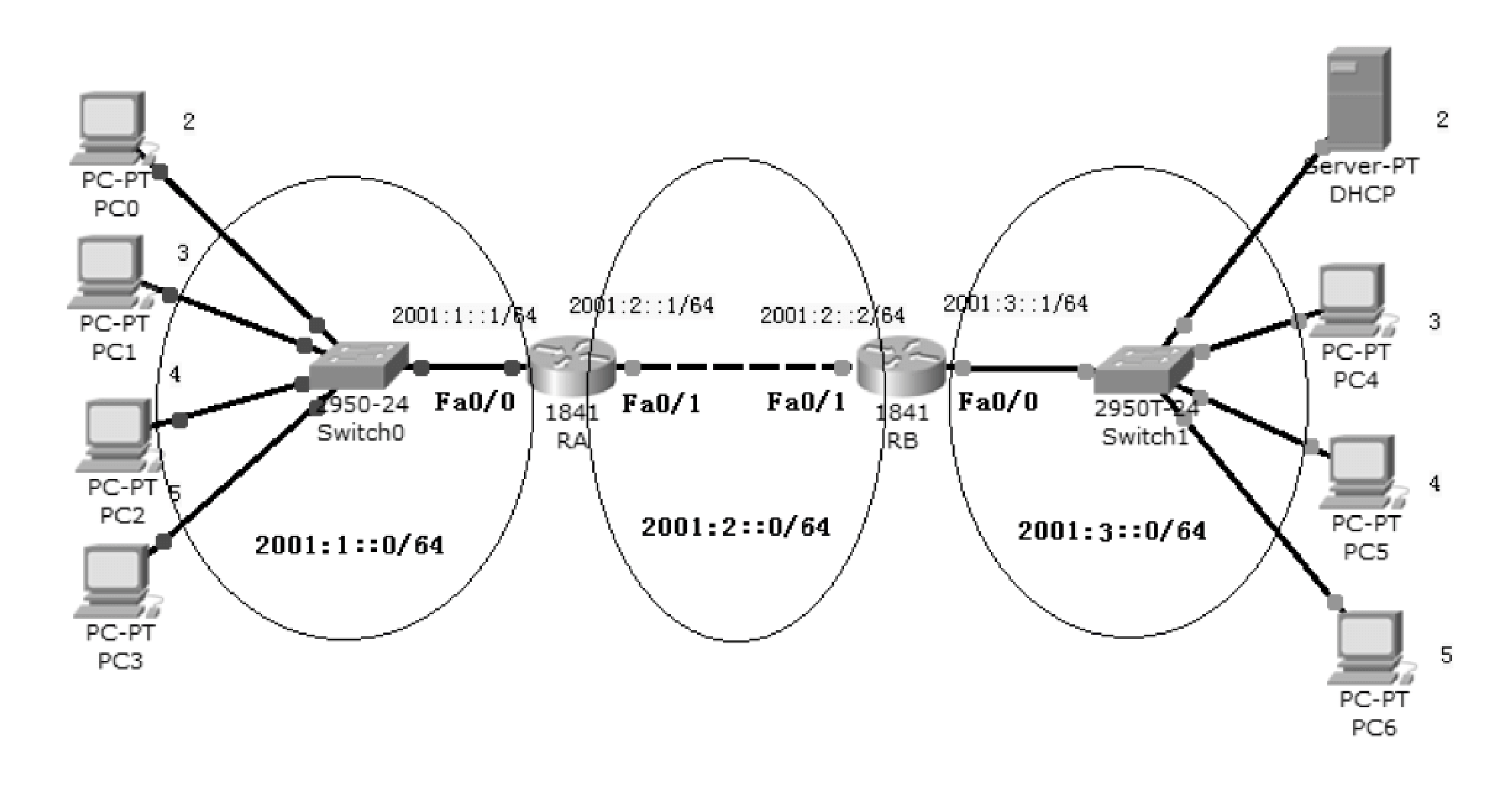
```
Router1（config-if）#ipv6 rip 1 enable
```

这将使该接口参与 RIP 进程 1 的活动，不必进入路由器全局配置使用 network 进行配置。

因此要记住，RIPng 的应用与在 IPv4 网络中基本一样。最大的不同是，它使用网络本身，而不是使用大家习惯了的网络命令，来启用接口到所连接的网络的路由功能。

示例：在 IPv6 网络中配置 RIPng

打开随书光盘中第 10 章练习“02　IPv6 动态路由协议 RIPng.pkt”，网络拓扑如图 10-12 所示。网络中有 3 个 IPv6 网段，计算机和路由器已经按照图示配置好了 IPv6 地址，你需要在 IPv6 环境中配置动态路由协议 RIPng。



▲图 10-12　IPv6 动态路由协议 RIPng 实验环境

配置 RIPng 的步骤如下。

（1）在 RA 上配置 RIPng。

```
RA（config）#ipv6 unicast-routing   --在路由器上启用 IPv6
RA （config）#ipv6 router rip ds    --启用 RIPng，后面的 ds 是 RIPng 进程名称，
  可以是数字和字符
RA （config-rtr）#exit
RA （config）#interface fastEthernet 0/0
RA （config-if）#ipv6 rip ds enable  --在该接口启用 RIPng，相当于 network 的作用
RA （config-if）#exit
RA （config）#interface fastEthernet 0/1
RA （config-if）#ipv6 rip ds enable
```

（2）在 RB 上配置 RIPng。

```
RB（config）#ipv6 unicast-routing   --在路由器上启用 IPv6
RB （config）#ipv6 router rip ds    --启用 RIPng，后面的 ds 是名称
RB （config-rtr）#exit
RB （config）#interface fastEthernet 0/0
RB （config-if）#ipv6 rip ds enable --在该接口启用 RIPng，相当于 network 的作用
```

```
RB (config-if) #exit
RB (config) #interface fastEthernet 0/1
RB (config-if) #ipv6 rip ds enable
```

（3）查看 RA 路由器的路由表。

```
RA#show ipv6 route
IPv6 Routing Table - 6 entries
C   2001:1::/64 [0/0]
     via ::, fastEthernet0/0
L   2001:1::1/128 [0/0]
     via ::, fastEthernet0/0
C   2001:2::/64 [0/0]
     via ::, fastEthernet0/1
L   2001:2::1/128 [0/0]
     via ::, fastEthernet0/1
R   2001:3::/64 [120/1]              --通过 RIPng 学到的路由
     via FE80::201:64FF:FE40:4E02, FastEthernet0/1
L   FF00::/8 [0/0]
     via ::, Null0
```

（4）在 RA 上查看运行的支持 IPv6 的路由协议。

```
RA#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static
IPv6 Routing Protocol is "rip ds"
  Interfaces:
    fastEthernet0/0
    fastEthernet0/1
```

（5）PC0 ping DHCP 服务器，能通。

```
PC>ping 2001:3::2
```

10.3.3 配置 EIGRPv6 支持 IPv6

就像 RIPng 一样，EIGRPv6 与其 IPv4 前辈几乎是一样的，EIGRP 的大多数特性在 EIGRPv6 中都保留了。

EIGRPv6 仍然是高级距离矢量路由协议，并且有一些链路状态路由协议的特征。邻居发现的过程仍然使用 hello 来进行，它仍然使用可靠的传输协议来提供可靠的通信，并使用弥散更新算法（DUAL）实现无环路的快速收敛。

EIGRPv6 使用组播传输来发送 hello 包和更新信息，正如 RIPng 一样，EIGRPv6 的组播地址几乎是一样的。在 IPv4 中，它是 224.0.0.10；在 IPv6 中，它是 FF02::A（在十六进制表示法中，A=10）。

但显然，这两个版本有着不同之处。最明显的不同是，正如 RIPng 一样，不使用网络命令了，要通告的网络和接口必须在接口配置模式下启用。但在 EIGRPv6 中，仍然使用路由器配置模式来启用路由协议，因为路由协议必须用文字命令打开，就像要用 no shutdown 命令打开接口一样。

EIGRPv6 的配置如下：

```
Router1 (config) #ipv6 router eigrp 10
```

在这里，10 仍然是自治系统（AS）号。提示符变成了（config-rtr） #，而且必须在这里执行 no shutdown 命令：

```
Router1 (config-rtr) #no shutdown
```

还必须指定一个 routerID：

```
Router1 (config-rtr) #router-id 4.0.0.1
```

在这种模式下，也可以配置其他的选项，比如路由再发布。

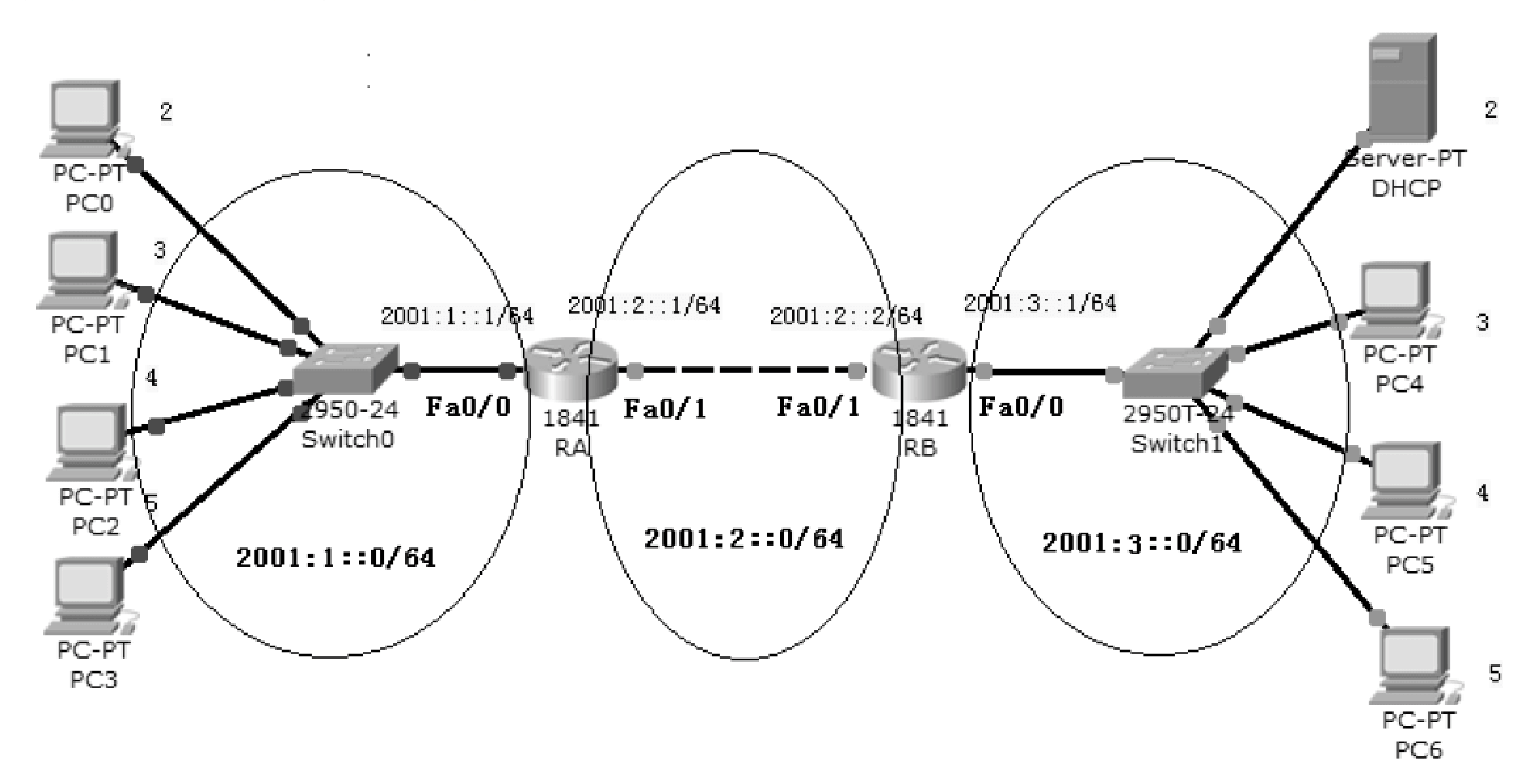
现在，让我们进入接口模式，并启用 EIGRPv6：

```
Router1 (config-if) #ipv6 eigrp 10
```

在接口命令中，10 同样表示 AS 号，它是在配置模式下启用的。

示例：在 IPv6 网络中配置 EIGRPv6

打开随书光盘中第 10 章练习“03 IPv6 动态路由协议 EIGRPv6.pkt”，网络拓扑如图 10-13 所示。网络中有 3 个 IPv6 网段，计算机和路由器已经按照图示配置好了 IPv6 地址，你需要在 IPv6 环境中配置动态路由协议 EIGRPv6。



▲图 10-13　IPv6 动态路由协议 EIGRPv6 实验环境

配置 EIGRPv6 的步骤如下。

（1）使用 PC0 ping DHCP 测试网络，你会发现不通。因为路由器没有配置路由表。

（2）在 RA 上启用 EIGRPv6。

```
RA（config）#ipv6 unicast-routing        --启用 IPv6 支持
RA（config）#ipv6 router eigrp 10        --10 是自制系统编号，和 EIGRP 一样
RA（config-rtr）#router-id 4.0.0.1       --指定一个 routerID，必须的
RA（config-rtr）#no shutdown             --必须运行 no shutdown 启用 EIGRP
RA（config-rtr）#exi
RA（config）#interface fastEthernet 0/0
RA（config-if）#ipv6 eigrp 10
                           --在接口启用 EIGRPv6，相当于 EIGRP 中的 network 作用
RA（config-if）#ex
RA（config）#interface fastEthernet 0/1
RA（config-if）#ipv6 eigrp 10
```

（3）在 RB 上启用 EIGRPv6。

```
RB（config）#ipv6 unicast-routing
RB（config）#ipv6 router eigrp 10
RB（config-rtr）#router-id 4.0.0.2  --指定一个 routerID，必须的
RB（config-rtr）#no shutdown         --必须运行 no shutdown 启用 EIGRP
RB（config-rtr）#exi
RB（config）#interface fastEthernet 0/0
RB（config-if）#ipv6 eigrp 10
RB（config-if）#ex
RB（config）#interface fastEthernet 0/1
RB（config-if）#ipv6 eigrp 10
```

（4）在 RB 上查看 IPv6 路由表。

```
RB#show ipv6 route
IPv6 Routing Table - 6 entries
D   2001:1::/64 [90/30720]             --通过 EIGRPv6 学到的路由
     via FE80::260:3EFF:FEC8:8402,  fastEthernet0/1
C   2001:2::/64 [0/0]
     via ::, fastEthernet0/1
L   2001:2::2/128 [0/0]
     via ::, fastEthernet0/1
C   2001:3::/64 [0/0]
     via ::, fastEthernet0/0
L   2001:3::1/128 [0/0]
     via ::, fastEthernet0/0
L   FF00::/8 [0/0]
```

```
      via ::, Null0
```

（5）在 RB 上查看支持 IPv6 的动态路由协议配置情况。

```
RB#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "eigrp 10 "
  EIGRP metric weight K1=1,K2=0,K3=1,K4=0,K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Interfaces:
    fastEthernet0/0
    fastEthernet0/1
Redistributing: eigrp 10
  Maximum path: 16
  Distance: internal 90 external 170
```

（6）使用 PC0 ping DHCP，你会发现网络通。

```
PC>ping 2001:3::2
```

10.3.4 配置 OSPFv3 支持 IPv6

新版本的 OSPF 与 IPv4 中的 OSPF 有许多相似之处。

OSPF 的基本概念还是一样的，它仍然是链路状态路由协议，它将整个网络或自治系统分成地区，从而使网络具有层次。

在 OSPFv2 中，路由器 ID（RID）由分配给路由器的最大 IP 地址决定（也可以由你来分配）。在 OSPFv3 中，可以分配 RID、地区 ID 和链路状态 ID，链路状态 ID 仍然是 32 位的值，但却不能再使用 IP 地址来找到了，因为 IPv6 的地址为 128 位。根据这些值的不同分配，会有相应的改动，从 OSPF 包的报头中，还删除了 IP 地址信息，这使得新版本的 OSPF 几乎能通过任何网络层协议进行路由。

在 OSPFv3 中，邻接和下一跳属性使用链路本地地址，但仍然使用组播流量来发送其更新和应答信息。对于 OSPF 路由器，地址为 FF02::5，对于 OSPF 指定路由器，地址为 FF02::6，这些新地址分别用来替换 224.0.0.5 和 224.0.0.6。

此外，IPv4 协议的灵活性不是太好，不具有通过 OSPFv2 向 OSPF 进程分配特定的网络和接口的能力。但仍然需要在路由器配置模式下配置一些选项。在 OSPFv3 中，就像我们前面讨论过的其他 IPv6 路由协议的配置一样，接口及与这些接口相连的网络，是在接口配置模式下直接在接口上进行配置的。

OSPFv3 的配置如下：

```
Router1（config）#ipv6 router ospf 10
```

```
Router1 (config-rtr) #router-id 4.0.0.1
```

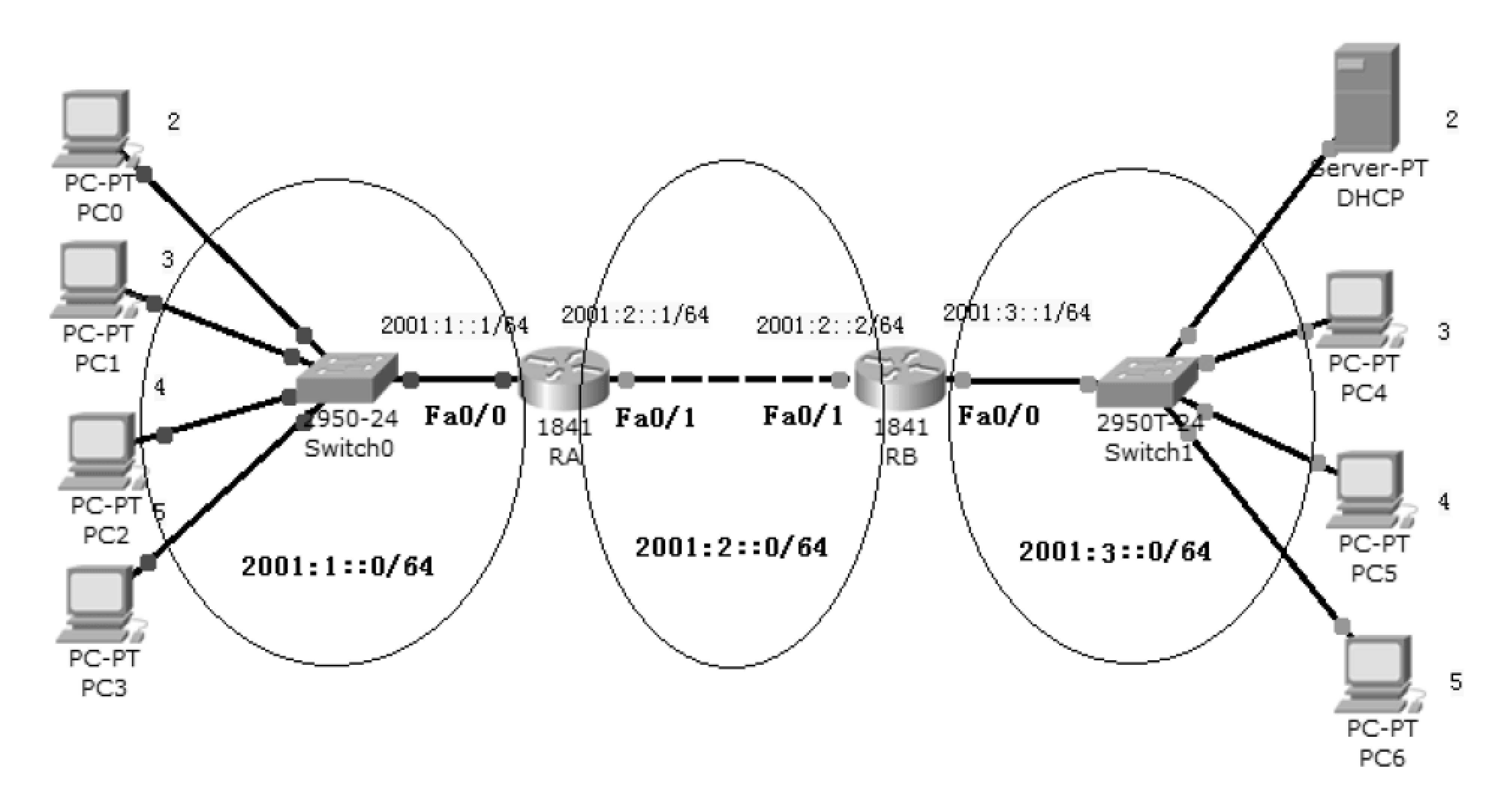
需要从路由器配置模式中执行一些配置命令，比如路由汇总和重分配。

在接口上启用 OSPFv3，只需进入每个接口并分配进程 ID 和地区即可。

```
Router1 (config-if) #ipv6 ospf 10 area 0
```

示例：在 IPv6 网络中配置 OSPFv3

打开随书光盘中第 10 章练习“04　IPv6 动态路由协议 OSPFv3.pkt”，网络拓扑如图 10-14 所示。网络中有 3 个 IPv6 网段，计算机和路由器已经按照图示配置好了 IPv6 地址，你需要在 IPv6 环境中配置动态路由协议 OSPFv3。



▲图 10-14　IPv6 动态路由协议 OSPFv3 实验环境

配置 OSPFv3 的步骤如下。

（1）在 RA 上启用 OSPFv3，并配置工作的接口和区域。

```
RA (config) #ipv6 unicast-routing
RA (config) #ipv6 router ospf 1      --1 是 OSPF 进程号
RA (config-rtr) #router-id 4.0.0.1   --指定一个 routerID 作为路由的标识，必须的
RA (config-rtr) #exit
RA (config) #interface fastEthernet 0/0
RA (config-if) #ipv6 ospf 1 area 0   --指定 OSPF 协议工作的接口和所属的区域
RA (config-if) #ex
RA (config) #interface fastEthernet 0/1
RA (config-if) #ipv6 ospf 1 area 0
```

（2）在 RB 上启用 OSPFv3，并配置工作的接口和区域。

```
RB (config) #ipv6 unicast-routing
RB (config) #ipv6 router ospf 1
RB (config-rtr) #router-id 4.0.0.2
```

```
RB (config-rtr) #ex
RB (config) #interface fastEthernet 0/0
RB (config-if) #ipv6 ospf 1 area 0
RB (config-if) #ex
RB (config) #interface fastEthernet 0/1
RB (config-if) #ipv6 ospf 1 area 0
```

（3）在 RB 上查看路由表。

```
RB#show ipv6 route
IPv6 Routing Table - 6 entries
O   2001:1::/64 [110/1]                    --通过 OSPFv3 学到的路由
     via FE80::260:3EFF:FEC8:8402, fastEthernet0/1
C   2001:2::/64 [0/0]
     via ::, fastEthernet0/1
L   2001:2::2/128 [0/0]
     via ::, fastEthernet0/1
C   2001:3::/64 [0/0]
     via ::, fastEthernet0/0
L   2001:3::1/128 [0/0]
     via ::, fastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

（4）在 RB 上查看配置 IPv6 的协议。

```
RB#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (area 0)
    fastEthernet0/0
    fastEthernet0/1
```

（5）使用 PC0 ping DHCP，测试 IPv6 网络是否畅通。

```
PC>ping 2001:3::2
```

10.4 IPv6 和 IPv4 共存

为了解决 IPv4 存在的问题，早在 1995 年，互联网工作组（IETF）就已经开始着手开发下一代互联网技术。于是 IPv6 应运而生。

在目前以 IPv4 为基础的网络技术如此成熟与成功的情况下，不可能马上抛开原有 IPv4 网络来创建 IPv6 网络，只能通过分步实施的方法来逐步过渡。因此，在今后相当长的一段时间内，IPv6 网络将和 IPv4 网络共存。如何以合理的代价逐步地将 IPv4 网络过渡到 IPv6、解决好 IPv4 与 IPv6 互相共存将是我们需要迫切考虑的。针对以上问题，目前提出了三种主要的过渡技术：双协议栈（DualStack）、隧道技术（Tunnel）、地址协议转换（NAT-PT）。当然，这些过渡技术都不是普遍适用的，每一种技术都是适用于某种或几种特定的网络情况，在实际应用时需综合考虑各方面现实情况，然后选择合适的转换机制进行设计和实施。

10.4.1 双协议栈技术

双协议栈是指在单个结点同时支持 IPv4 和 IPv6 两种协议。由于 IPv6 和 IPv4 是功能相近的网络层协议，两者都基于相同的物理平台，而且加载于其上的传输层协议 TCP 和 UDP 也没有区别，所以可以在一台主机上同时支持 IPv4 协议和 IPv6 协议。双协议栈技术的工作原理如下。

一台主机同时支持 IPv6 和 IPv4 两种协议，该主机既能与支持 IPv4 协议的主机通信，又能与支持 IPv6 协议的主机通信。双协议栈是其他 IPv4/IPv6 互通技术的基础，它有以下 3 种工作模式。

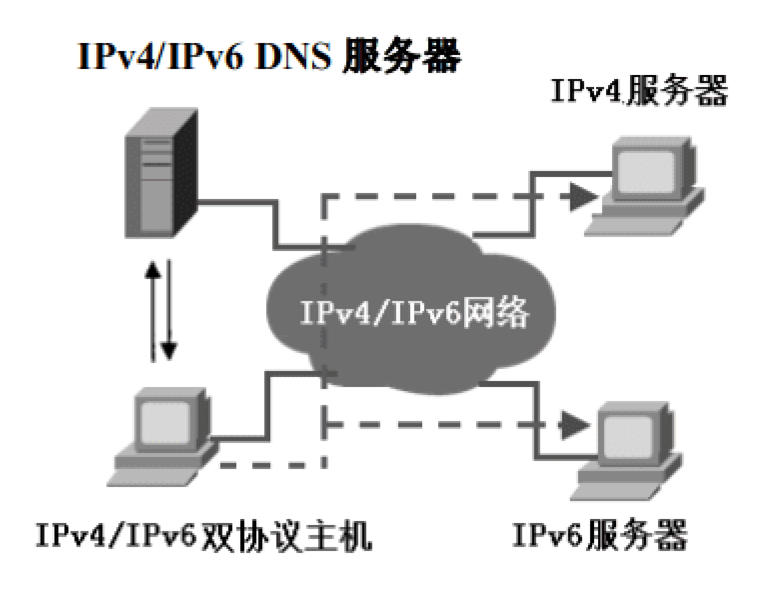
- 只运行 IPv6 协议，此时表现为 IPv6 结点。
- 只运行 IPv4 协议，此时表现为 IPv4 结点。
- 同时打开 IPv6 和 IPv4 协议。

双协议栈主机的协议结构如表 10-2 所示。

表 10-2 双协议栈主机的协议结构

<table>
<tr><th colspan="2">应用程序</th></tr>
<tr><td colspan="2">TCP/UDP 协议</td></tr>
<tr><td>IPv6 协议</td><td>IPv4 协议</td></tr>
<tr><td colspan="2">接入网络</td></tr>
</table>

双协议栈主机在通信时首先通过支持双协议的 DNS 服务器查询与目的主机名对应的 IP 地址，然后根据指定的 IPv6 或 IPv4 地址开始通信。双协议栈通信方式如图 10-15 所示。



▲图 10-15 双协议栈示意图

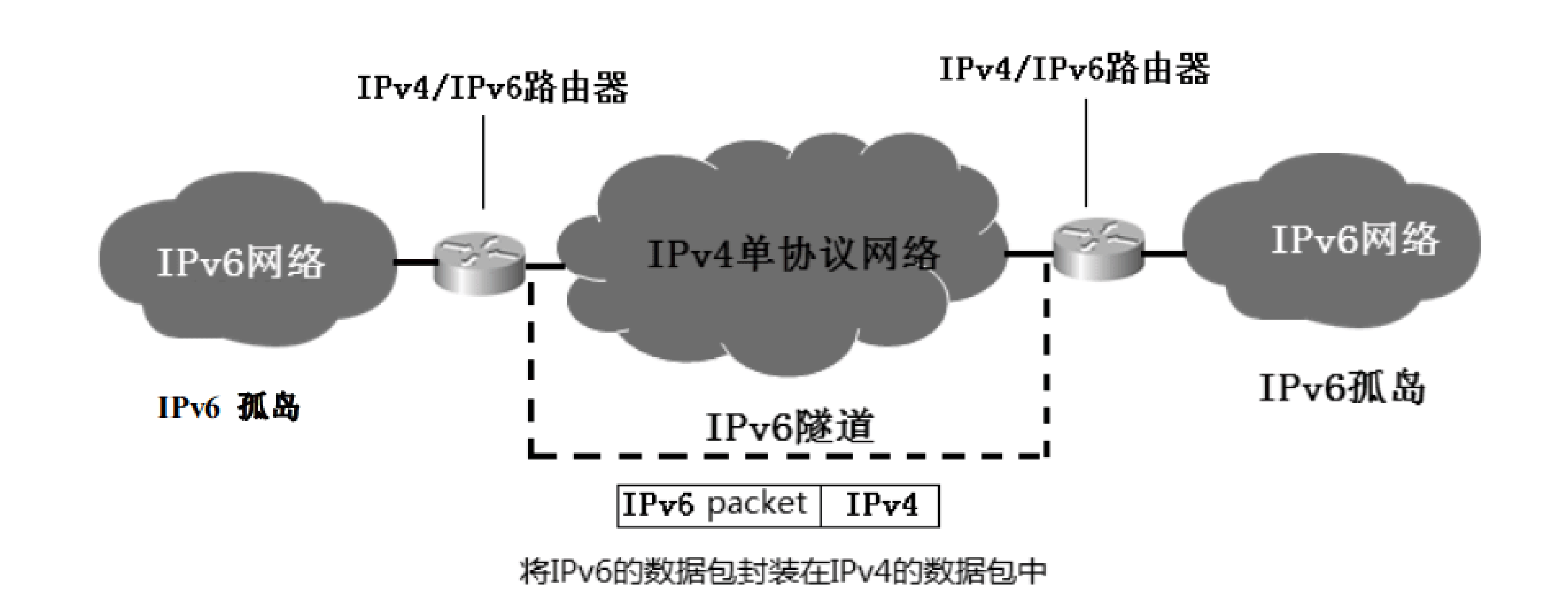
Windows Server 2008 和 Windows Server 2003 默认是双协议栈，Windows Server 2008 的 DNS 服务器支持 IPv4 和 IPv6 的名称解析。

10.4.2 6 to 4 隧道技术

隧道技术是将 IPv6 的报文分组封装到 IPv4 的分组中，分组的源地址和目的地址分别是隧道入口和出口的 IPv4 地址。

随着 IPv6 网络的发展，将会出现许多局部的 IPv6 网络，但是这些 IPv6 网络被运行 IPv4 协议的主干网络所分隔开来。IPv6 网络就像是处于 IPv4“海洋”中的“孤岛”，为了使这些“IPv6 孤岛”可以互通，必须使用隧道技术，此技术要求隧道两端的结点（路由器） 都支持 IPv4/IPv6 两种协议，其通信方式如图 10-16 所示。

在隧道的入口处，路由器将 IPv6 的数据报封装入 IPv4 中，IPv4 数据报的源地址和目的地址分别是隧道入口和出口的 IPv4 地址。在隧道的出口处再将 IPv6 数据报取出转发给目的站点。隧道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，因而很容易实现。但是隧道技术不能实现 IPv4 主机和 IPv6 主机的直接通信。



▲图 10-16　6 to 4 隧道示意图

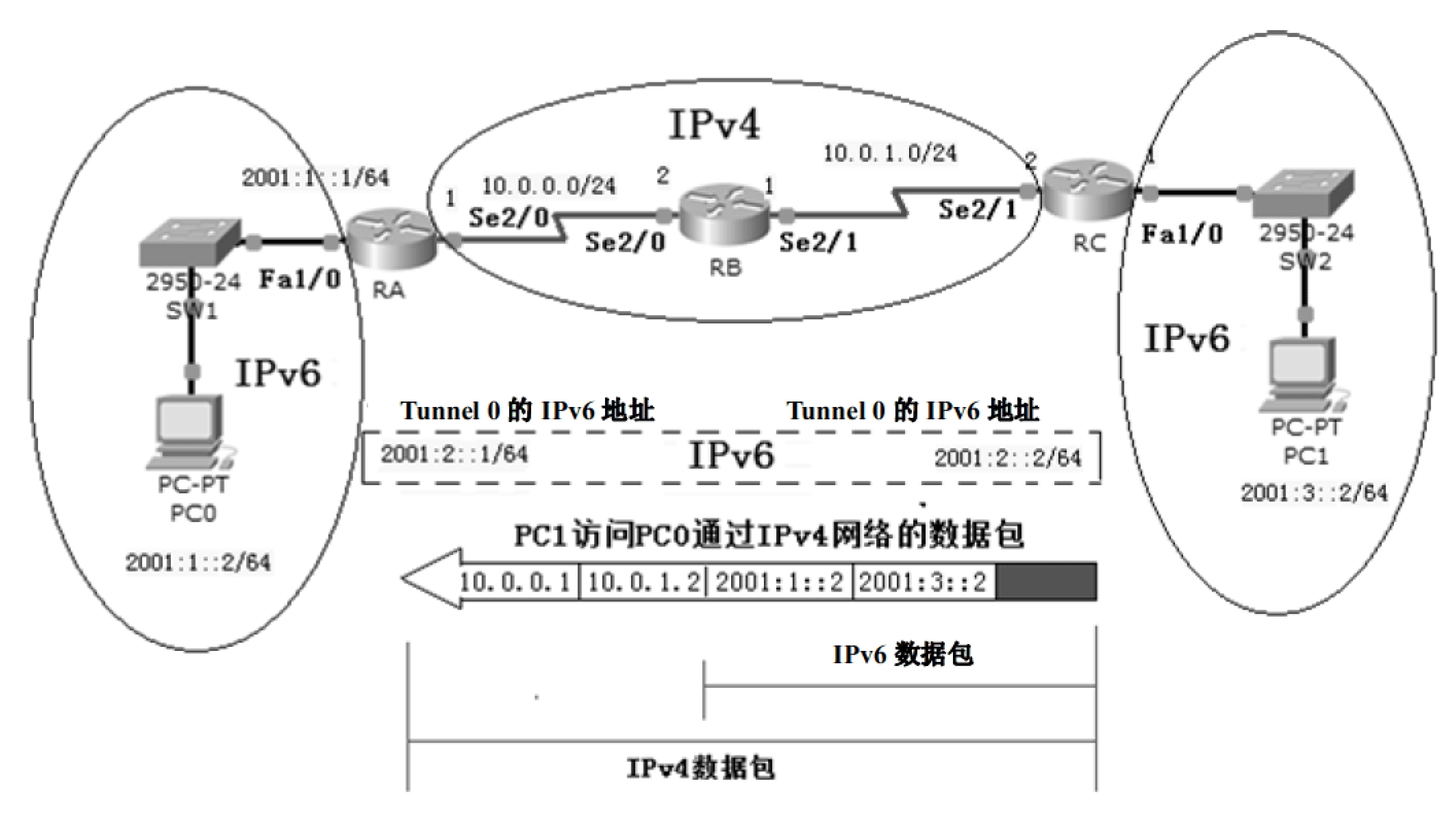
示例：配置 6 to 4 隧道

本实验使用 Dynamips 软件来运行 Cisco 3640 系列路由器 IOS。Packet Tracer 不支持该实验。该 IOS 从 www.91xueit.com 网站下载，文件名为 unzip-c3640-js-mz.124-10.bin。

6 to 4 隧道技术实验网络拓扑如图 10-17 所示。两个 IPv6 网络使用 IPv4 网络连接，网络中的计算机和路由器需要按照图示的地址配置 IPv6 地址和 IPv4 地址，需要在 RA 路由器上添加到 10.0.1.0/24 网段的路由，在 RC 路由器上添加到 10.0.0.0/24 网段的路由。

现在你需要在 RA 和 RC 路由器上配置一个 6 to 4 的隧道，将 IPv6 的数据包封装在 IPv4 的数据包中，使得两个 IPv6 的网络能够相互通信。

在配置 IPv6 隧道时，两端的 Tunnel0 接口也要配置 IPv6 地址。这两个 IPv6 地址必须在一个网段，这样你的 IPv6 网络就可以认为有 3 个网段，如图 10-17 所示。要想使这 3 个 IPv6 网络通，必须在 RA 和 RC 路由器上添加到对方网络的 IPv6 路由。



▲图 10-17　6 to 4 隧道实验环境

配置 6 to 4 隧道的步骤如下。

（1）在 RA 上的配置：

```
RA#config t
RA (config) #interface Tunnel ?        --配置隧道接口，查看可用的隧道接口数量
  <0-2147483647>  Tunnel interface number
RA (config) #interface Tunnel 0
RA (config-if) #no sh
RA (config-if) #ipv6 address 2001:2::1/64
RA (config-if) #Tunnel source 10.0.0.1
RA (config-if) #Tunnel destination 10.0.1.2
RA (config-if) #Tunnel mode ipv6ip
RA (config-if) #exit
RA (config) #ipv6 route 2001:3::/64 2001:2::2
```

最后一条命令添加到达 2001:3::0/64 网段的路由，下一跳是 RC 路由器 Tunnel 0 接口的 IPv6 地址。

（2）在 RC 上的配置：

```
RC#config t
RC (config) #interface Tunnel 0
RC (config-if) #no shutdown
RC (config-if) #ipv6 address 2001:2::2/64
RC (config-if) #Tunnel source 10.0.1.2
RC (config-if) #Tunnel destiNATion 10.0.0.1
RC (config-if) #Tunnle mode ipv6ip
```

```
RC (config-if) #exit
RC (config) #ipv6 route 2001:1::/64 2001:2::1  --这条命令添加到达 2001:1::0/64
                                  网段的路由，下一条是 RA 路由器 Tunnel0 接口的 IPv6 地址
RC#show ipv6 interface brief    --显示 IPv6 的配置，如图 10-18 所示
```

```
RC#show ipv6 interface brief
FastEthernet0/0            [administratively down/down]
    unassigned
FastEthernet0/1            [administratively down/down]
    unassigned
FastEthernet1/0            [up/up]
    FE80::CE00:DFF:FEC0:10
    2001:3::1
Serial2/0                  [administratively down/down]
    unassigned
Serial2/1                  [up/up]
    unassigned
Serial2/2                  [administratively down/down]
    unassigned
Serial2/3                  [administratively down/down]
    unassigned
Tunnel0                    [up/up]
    FE80::A00:102
    2001:2::2
```

▲图 10-18　显示接口 IPv6 地址

（3）在 RA 上 ping RC 的 Fa0/0 的 IPv6 地址，能通。

```
RA#ping 2001:3::1
```

10.4.3　ISATAP 隧道

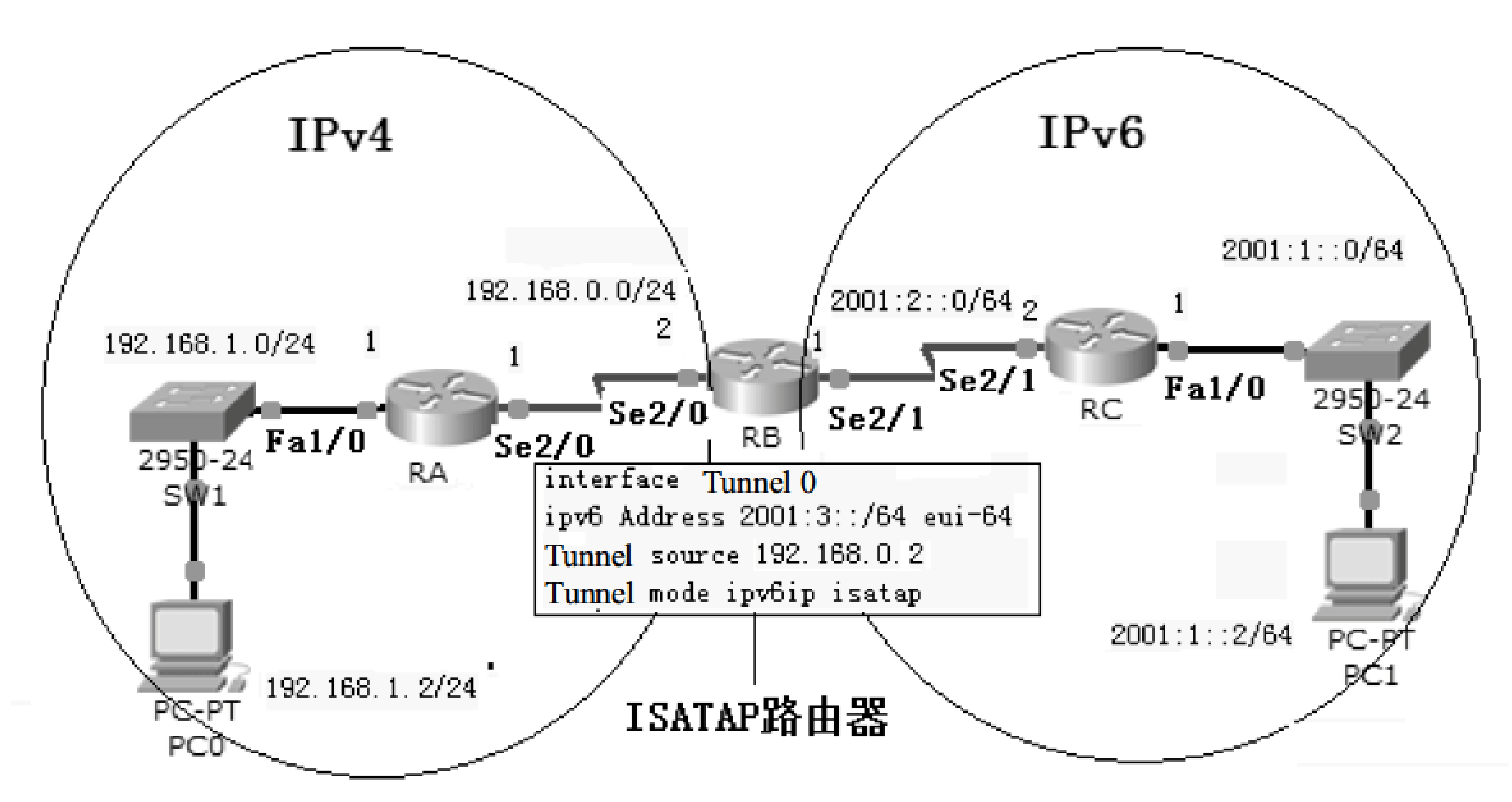
ISATAP（ Intra-Site Automatic Tunnel Addressing Protocol，站间自动隧道寻址协议）是一种地址分配和主机到主机、主机到路由器和路由器到主机的自动隧道技术。它为 IPv6 主机之间提供了跨越 IPv4 内部网络的单播 IPv6 连通性。ISATAP 一般用于 IPv4 网络中的 IPv6/IPv4 结点间的通信。ISATAP 使用本地管理的接口标识符::0:5EFE:w.x.y.z，其中，0:5EFE 部分是由 Internet 号码分配中心（IANA）所分配的机构单元标识符（00-00-5E）和表示内嵌的 IPv4 地址类型的类型号（FE）组合而成的；w.x.y.z 部分是任意的单播 IPv4 地址，既可以是私有地址，也可以是公共地址。

任何有效的 IPv6 单播地址的 64 位前缀都可以和 ISATAP 接口标识符相结合。它们包括链路本地地址前缀（FE80::/64）、全球前缀（包括 6 to 4 前缀）和站点本地前缀。

ISATAP 地址中也包含了一个内嵌的 IPv4 地址，这一点与 IPv4 映射地址、6 over 4 地址和 6 to 4 地址类似。内嵌的 IPv4 地址的作用是：在发往 ISATAP 地址的 IPv6 通信流通过隧道跨越了 IPv4 网络后，可用它来确定 IPv4 报头中的源 IPv4 地址或目标 IPv4 地址。

示例：配置 ISATAP 隧道

本实验使用 Dynamips 软件创建的网络环境进行配置，Packet Tracer 不支持本实验。网络拓扑如图 10-19 所示，按照图示配置网络中路由器的 IPv4 地址和 IPv6 地址，并添加路由表使 IPv4 的网络能够畅通。



PC0到PC1使用PC0的IPv4地址作为源IP地址，ISATAP路由器的IPv4地址作为目标IP地址
去掉IPv4的数据包头进入IPv6网络

2001:3::5efe.192.168.1.2 | 2001:1::2 | 192.168.1.2 | 192.168.0.2 → 2001:3::5efe.192.168.1.2 | 2001:1::2 →

← 192.168.1.2 | 192.168.0.2 | 2001:3::5efe.192.168.1.2 | 2001:1::2 ← 2001:3::5efe.192.168.1.2 | 2001:1::2

从IPv6的数据包提取出IPv4的地址作为目标地址，Tunnel Source地址作为IPv4的源地址
将IPv6的数据包封装到IPv4的数据包中 进入IPv4的网络

▲图 10-19　ISATAP 隧道实验环境

注意	IPv4 网络不能有网络地址转换，否则会失败。

实验步骤如下。

（1）在 RA 路由器上的配置：

```
RA#configt
RA (config) #interface Serial 2/0
RA (config-if) #clock rate 64000
RA (config-if) #ip address 192.168.0.1 255.255.255.0
RA (config-if) #no sh
RA (config-if) #ex
RA (config) #interface Fa 1/0
RA (config-if) #ip address 192.168.1.1 255.255.255.0
RA (config-if) #no sh
```

（2）在 RB 路由器上的配置：

```
RB (config) #ipv6 unicast-routing
RB (config) #interface Serial 2/1
RB (config-if) #clock rate 64000
```

```
RB (config-if) #ipv6 address 2001:2::1/64
RB (config-if) #no sh
RB (config-if) #ex
RB (config) #interface Serial 2/0
RB (config-if) #ip address 192.168.0.2 255.255.255.0
RA (config-if) #no sh
RB (config-if) #ex
RB (config) #ipv6 route 2001:1::/64 2001:2::2
                                --添加到达 2001:1:: /64 网段的路由
RB (config) #ip route 192.168.1.0 255.255.255.0 192.168.0.1
```

（3）在 RB 上配置 ISATAP 接口。

```
RB (config) #interface Tunnel0
RB (config-if) #ipv6 address 2001:3::/64 eui-64
                                --注意 IPv6 的必须使用 eui-64 方式指定
RB (config-if) #no ipv6 nd suppress-ra
                                --在 IPv6 的接口上将不会发送路由器公告报文
RB (config-if) #Tunnel Source 192.168.0.2
RB (config-if) #Tunnel mode ipv6ip ?
  6to4         IPv6 automatic tunnelling using 6to4
  auto-tunnel  IPv6 automatic tunnelling using IPv4 compatible addres
  isatap       IPv6 automatic tunnelling using ISATAP
  <cr>
RB (config-if) #tunnel mode ipv6ip isatap
RB (config-if) #no sh
```

必须使用 eui 方式指定 Tunnel 0 接口的 IPv6 地址。

配置了一个 Interface Tunnel 0，为该接口配置了一个 IPv6 地址，并且指定了隧道的源地址，并配置隧道模式为 ISATAP。现在 ISATAP 路由器就配置好了，下面配置 IPv6 网络中的计算机 PC0，指定 ISATAP 路由器的地址 192.168.0.2，ISATAP 路由器则会为 PC0 分配一个 IPv6 地址 2001:3::5efe:192.168.0.2，IPv4 的计算机都会被分配到 2001:3::/63 网段。

（4）在 RB 路由器上查看运行的配置。

```
RB#show running-config   --可以看到 interface Tunnel0 的配置，以下是部分输出
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2001:3::/64 eui-64
 no ipv6 nd suppress-ra
 tunnel source 192.168.0.2
```

```
 tunnel mode ipv6ip isatap
!
```

（5）在 RC 上的配置，配置隧道。

```
RC (config) #ipv6 unicast-routing
RC (config) #interface fastEthernet 1/0
RC (config-if) #ipv6 address 2001:1::1/64
RC (config-if) #no sh
RC (config-if) #ex
RC (config) #interface Serial 2/1
RC (config-if) #ipv6 address 2001:2::2/64
RC (config-if) #clock rate 64000
RC (config-if) #no sh
RC (config) #ipv6 route 2001:3::/64 2001:2::1
                        --添加到达 2001:3::/64 网段的路由
```

（6）在 IPv4 的计算机上配置 ISATAP 隧道。

ISATAP 客户端可以是 Windows XP、Windows Server 2003、Windows 7、Windows Server 2008。Windows Server 2003、Windows 7、Windows Server 2008 默认已经启用了 IPv6。Windows XP 需要安装 IPv6 协议，才能配置 ISATAP 隧道。必须保证 Windows XP 计算机能够和 ISATAP 路由器的接口 Se2/0 通信。

如图 10-20 所示，在命令提示符下，输入 ipconfig，能够看到 IPv6 的本地链路地址。

```
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.122
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::20c:29ff:fec5:1f77%5
        Default Gateway . . . . . . . . . : 192.168.1.1      本地链路地址

Tunnel adapter Teredo Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::ffff:ffff:fffd%4
        Default Gateway . . . . . . . . . :

Tunnel adapter Automatic Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::5efe:192.168.1.122%2
        Default Gateway . . . . . . . . . :
```

▲图 10-20　配置 IPv6 地址

在命令提示符下 ping RB 路由器的 IPv4 地址。确保能够 ping 通。

在命令提示符下输入以下命令，为计算机配置 ISATAP 隧道。

C:\ >netsh interface ipv6 ISATAP set router 192.168.0.2

如图 10-21 所示，指定 ISATAP 路由器地址，ISATAP 路由器就会分配给计算机一个路由器前缀，所有配置了 ISATAP 隧道的计算机都会分配到一个 IPv6 网段，也就是和 ISATAP 路由器的 Tunnel 0 接口在同一个网段。

```
C:\Documents and Settings\Administrator>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=24ms TTL=254
Reply from 192.168.0.2: bytes=32 time=20ms TTL=254
Reply from 192.168.0.2: bytes=32 time=24ms TTL=254
Reply from 192.168.0.2: bytes=32 time=24ms TTL=254

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 24ms, Average = 17ms

C:\Documents and Settings\Administrator>cd \

C:\>netsh interface ipv6 isatap set router 192.168.0.2
确定。
```

▲图 10-21　配置 ISATAP 隧道

如图 10-22 所示，再次输入 ipconfig，你能看到 ISATAP 路由器配置给计算机的 IPv6 地址，可以看到该地址是 2001:3::+ 5efe + IPv4 地址构成的。如果没有出现自动配置的 2001:3::网段，禁用、启用网卡即可解决。

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.122
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::20c:29ff:fec5:1f77%5
        Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::ffff:ffff:fffd%4
        Default Gateway . . . . . . . . . :

Tunnel adapter Automatic Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 2001:3::5efe:192.168.1.122
        IP Address. . . . . . . . . . . . : fe80::5efe:192.168.1.122%2
        Default Gateway . . . . . . . . . : fe80::5efe:192.168.0.1%2
```

▲图 10-22　ISATAP 路由器分配给计算机的 IPv6 地址

（7）使用配置了 ISATAP 隧道的 IPv4 网络中的计算机测试到 IPv6 网络的连通性。使用网络拓扑中的 PC0 ping RC 路由器的 Fa1/0 接口。

```
C:\>ping 2001:1::1
Pinging 2001:1::1 with 32 bytes of data:
Reply from 2001:1::1: time=11ms
Reply from 2001:1::1: time=1ms
```

```
Reply from 2001:1::1: time=2ms
Reply from 2001:1::1: time=1ms
Ping statistics for 2001:1::1:
   Packets: Sent = 4,Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 11ms, Average = 3ms
```

到目前为止，IPv4 网络中的计算机能访问 IPv6 网络中的计算机。

10.4.4 NAT-PT

NAT-PT 技术是通过与 SIIT 协议转换和传统的 IPv4 下的动态地址翻译及应用层网关相结合，实现只安装 IPv6 的计算机和只安装 IPv4 的计算机通信。NAT-PT 是最常用的协议转换技术，它通过 SIIT 协议转换技术和 IPv4 网络中的动态地址翻译（NAT）技术适当地与应用层网关（Application Level Gateway，ALG）相结合，实现了 IPv6 主机和纯 IPv4 主机的大部分应用的相互通信。

NAT-PT 通过 IPv4 和 IPv6 数据包之间报头和语义的翻译为 IPv6 结点与 IPv4 结点之间的通信提供透明的路由。它采用传统的 IPv4 下的 NAT 技术来分配 IPv4 地址，这样就可以用很少的 IPv4 地址构成自己的 IPv4 地址分配池，可以给大量的需要进行地址转换的应用使用协议转换技术服务。

NAT-PT 可以分为静态和动态模式。

1）静态 NAT-PT

静态模式提供一对一的 IPv6 地址和 IPv4 地址的映射。IPv6 单协议网络域内的结点要访问 IPv4 单协议网络域内的每一个 IPv4 地址，都必须在 NAT-PT 设备中配置。每一个目的 IPv4 在 NAT-PT 设备中被映射成一个具有预定义 NAT-PT 前缀的 IPv6 地址。在这种模式下，每一个 IPv6 映射到 IPv4 地址需要一个源 IPv4 地址。

2）动态 NAT-PT

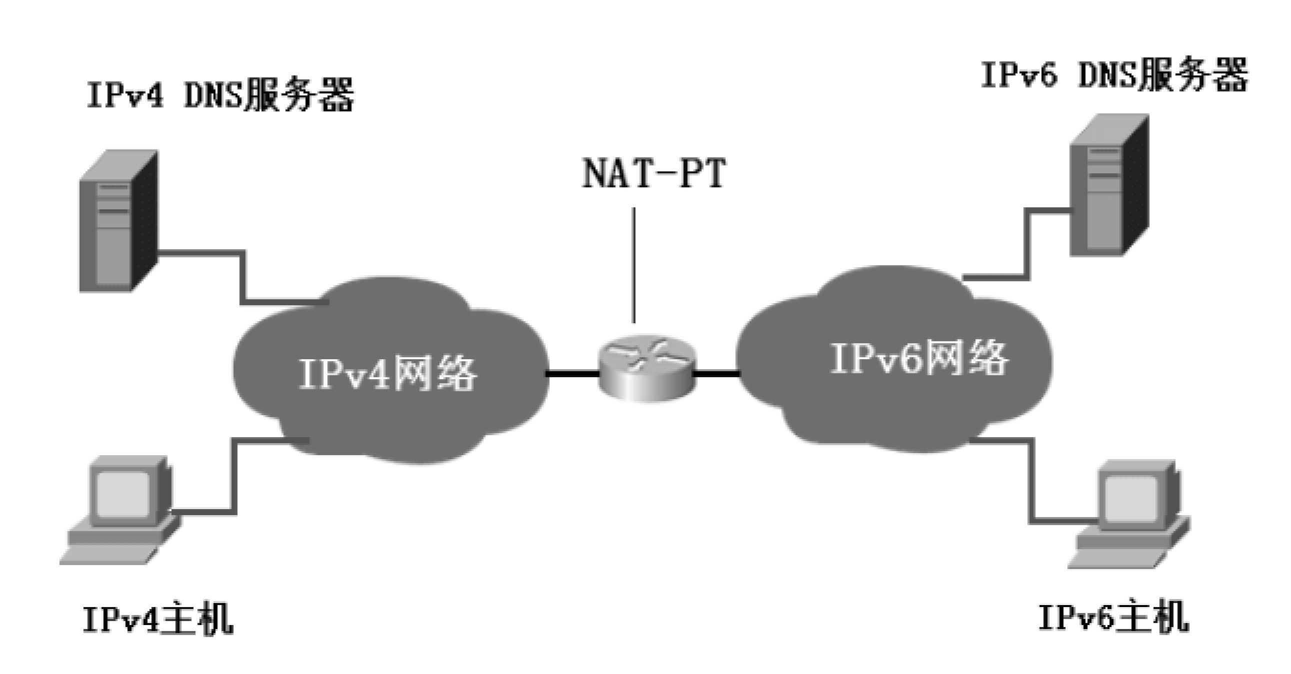
在动态 NAT-PT 中，NAT-PT 网关向 IPv6 网络通告一个 96 位的地址前缀，并结合主机 32 位 IPv4 地址作为对 IPv4 网络中主机的标识。从 IPv6 网络中的主机向 IPv4 网络发送的报文，其目的地址前缀与 NAT-PT 发布的地址前缀相同，这些报文都被路由到 NAT-PT 网关，由 NAT-PT 网关对报文头进行修改，取出其中的 IPv4 地址信息，替换目的地址。同时，NAT-PT 网关定义了 IPv4 地址池，它从地址池中取出一个地址来替换 IPv6 报文的源地址，从而完成从 IPv6 地址到 IPv4 地址的转换。

动态 NAT-PT 改进了静态 NAT-PT 配置复杂、消耗大量 IPv4 地址池的缺点。由于它采用上层协议映射方法，故只需用很少的 IPv4 地址就可以支持大量的 IPv6 到 IPv4 的转换。但是，动态 NAT-PT 只能由 IPv6 一侧首先发起连接，路由器把 IPv6 地址转换为 IPv4 地址后，IPv4 主机才知道使用哪一个 IPv4 地址来标识 IPv6 主机。若从 IPv4 端首先发起连接，

IPv4 主机并不知道 IPv6 主机的 IPv4 地址，因为这个地址是 NAT-PT 网关从地址池中随机选择的，连接将无法进行。

3）结合 ALG 的动态 NAT-PT

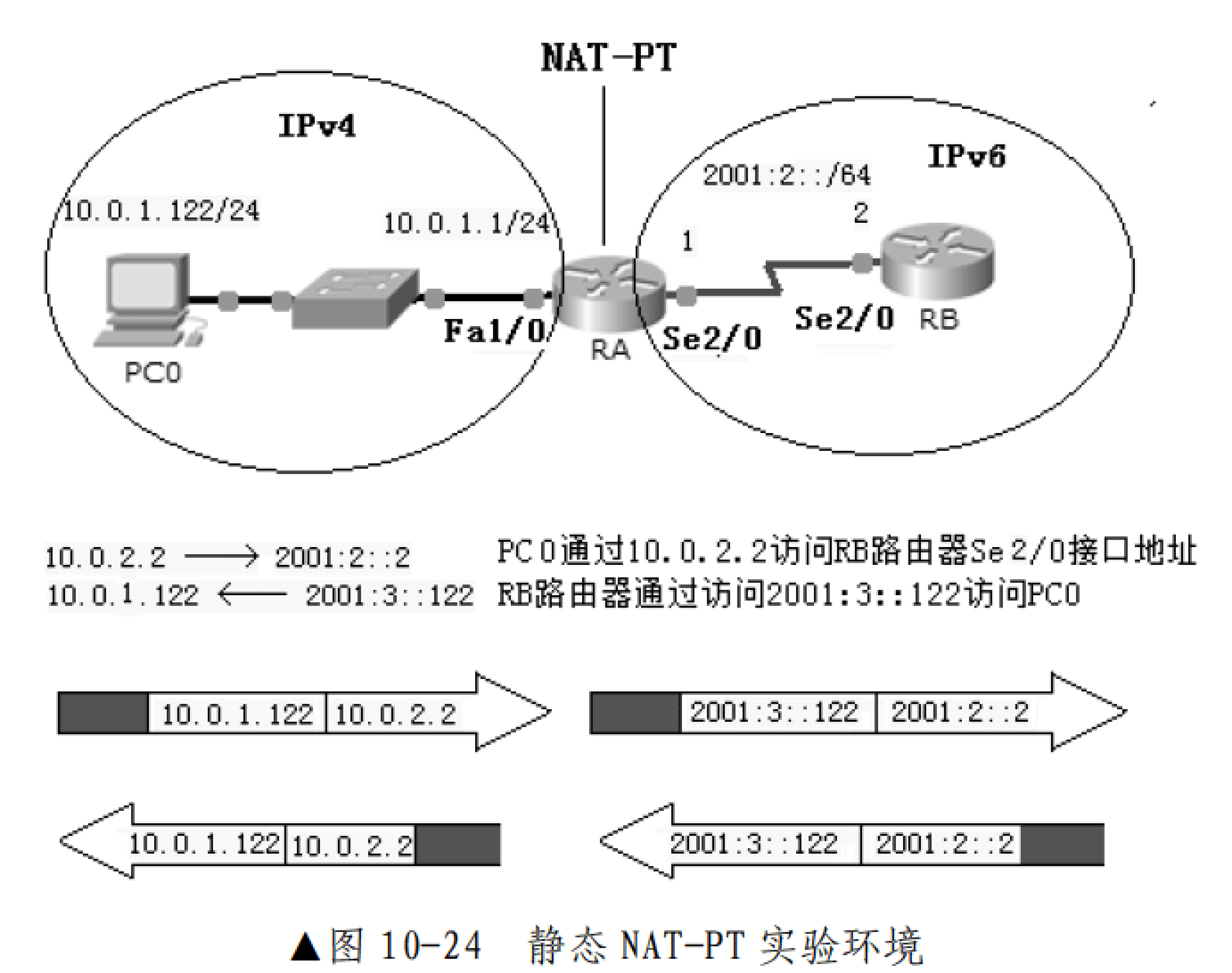
ALG 即应用层网关，如图 10-23 所示。动态 NAT-PT 映射可以和 DNS ALG 联合使用来转换 DNS 传输，以自动建立目的结点的转换地址。NAT-PT 可以截取由 IPv6 网络发往 IPv4 网络的 DNS 请求（A 记录查询）。IPv6 网络内的 DNS 服务器必须通过 NAT-PT 设备首先向 IPv4 的 DNS 服务器发送 DNS 查询，随后 NAT-PT 自动地将 DNS 响应（A 记录）内容转换为一个 IPv6 地址（A6 记录），外部 IPv4 地址和有 NAT-PT 前缀的 IPv6 地址的 NAT-PT 映射被动态的配置。然后，IPv6 单协议网络结点就可以从 NAT-PT 设备获得一个可以到达 IPv4 目的的 IPv6 地址。



▲图 10-23　应用程序网关

1．示例：配置静态 NAT-PT

本实验使用的 IOS 是 unzip-c3640-js-mz.124-10.bin，下载网址 http://www.91xueit.com，使用 Dynamips 软件搭建的实验环境，网络拓扑如图 10-24 所示，PC0 使用 Windows XP 模拟，IPv4 的地址为 10.0.1.122，网关为 10.0.1.1，RA 路由器 Fa1/0 接口的 IPv4 地址为 10.0.1.1，Se2/0 接口的 IPv6 的 IP 地址为 2001:2::1，RB 路由器的接口 Se2/0 为 2001:2::2。



▲图 10-24　静态 NAT-PT 实验环境

实验目标：现在需要在路由器 RA 上配置 NAT-PT 静态映射，使得 PC0 能够 ping 通路由器 RB 的 Se2/0 接口。配置静态映射的结果是：PC0 通过访问 10.0.2.2 访问路由器 RB 的 Se2/0 接口 IPv6 地址，路由器 RB 通过访问 2001:3::122 访问 PC0 的 IPv4 地址。

配置静态 NAT-PT 的步骤如下。

（1）在 RA 上配置静态 NAT-PT。

```
RA（config）#ipv6 unicast-routing
RA（config）#interface fastEthernet 1/0
RA （config-if）#ip address 10.0.1.1 255.255.255.0
RA （config-if）#no shutdown
RA（config-if）#ipv6 NAT
RA（config-if）#exit
RA（config）#interface Serial 2/0
RA（config-if）#clock rate 64000
RA（config-if）#no shutdown
RA（config-if）#ipv6 address 2001:2::1/64
RA（config-if）#ipv6 NAT
RA（config-if）#exit
RA（config）#ipv6 NAT v6v4 source 2001:2::2 10.0.2.2
                --该命令使 IPv4 的计算机通过访问 10.0.2.2 就能够访问到 2001:2::2
RA（config）#ipv6 NAT v4v6 source 10.0.1.122 2001:3::122
--该命令使 IPv6 的计算机通过访问 2001:3::122 就能访问到 10.0.1.122
RA（config）#ipv6 NAT prefix 2001:3::/96
     --定义前缀长度，必须是 96 位，这就意味着 IPv4 中的计算机都被映射到 IPv6 网络中的
        2001:3::/96 网段中
RA（config）#exit
RA#debug ipv6 NAT   --启用 IPv6 NAT 的事件输出
```

（2）在 RB 上，配置接口 IPv6 地址和添加 IPv6 路由。

```
RB（config）#ipv6 unicast-routing
RB（config）#interface Se 2/0
RB（config-if）#no shutdown
RB（config-if）#ipv6 address 2001:2::2/64
RB（config-if）#exit
RB（config）#ipv6 route ::/0 2001:2::1      --添加 IPv6 的默认路由
```

（3）在 PC0 上 ping 10.0.2.2，通过这个地址能够 ping 通 2001:2::2。

（4）在 RA 上可以看到 NAT-PT 的输出，如图 10-25 所示。

```
RA#debug ipv6 nat
IPv6 NAT-PT debugging is on
RA#
*Mar  1 00:27:58.183: IPv6 NAT:  src (10.0.1.122) -> (2001:3::122), dst (10.0.2.
2) -> (2001:2::2)
*Mar  1 00:27:58.279: IPv6 NAT: icmp src (2001:2::2) -> (10.0.2.2), dst (2001:3:
:122) -> (10.0.1.122)
*Mar  1 00:27:58.831: IPv6 NAT:  src (10.0.1.122) -> (2001:3::122), dst (10.0.2.
2) -> (2001:2::2)
*Mar  1 00:27:58.903: IPv6 NAT: icmp src (2001:2::2) -> (10.0.2.2), dst (2001:3:
:122) -> (10.0.1.122)
*Mar  1 00:27:59.527: IPv6 NAT:  src (10.0.1.122) -> (2001:3::122), dst (10.0.2.
2) -> (2001:2::2)
*Mar  1 00:27:59.599: IPv6 NAT: icmp src (2001:2::2) -> (10.0.2.2), dst (2001:3:
:122) -> (10.0.1.122)
*Mar  1 00:28:00.223: IPv6 NAT:  src (10.0.1.122) -> (2001:3::122), dst (10.0.2.
2) -> (2001:2::2)
*Mar  1 00:28:00.319: IPv6 NAT: icmp src (2001:2::2) -> (10.0.2.2), dst (2001:3:
:122) -> (10.0.1.122)
```

▲图 10-25　IPv6 NAT-PT 输出

（5）在 RB 上输入 debug ipv6 packet，可以看到 IPv6 数据包接收和转发产生的输出，如图 10-26 所示。

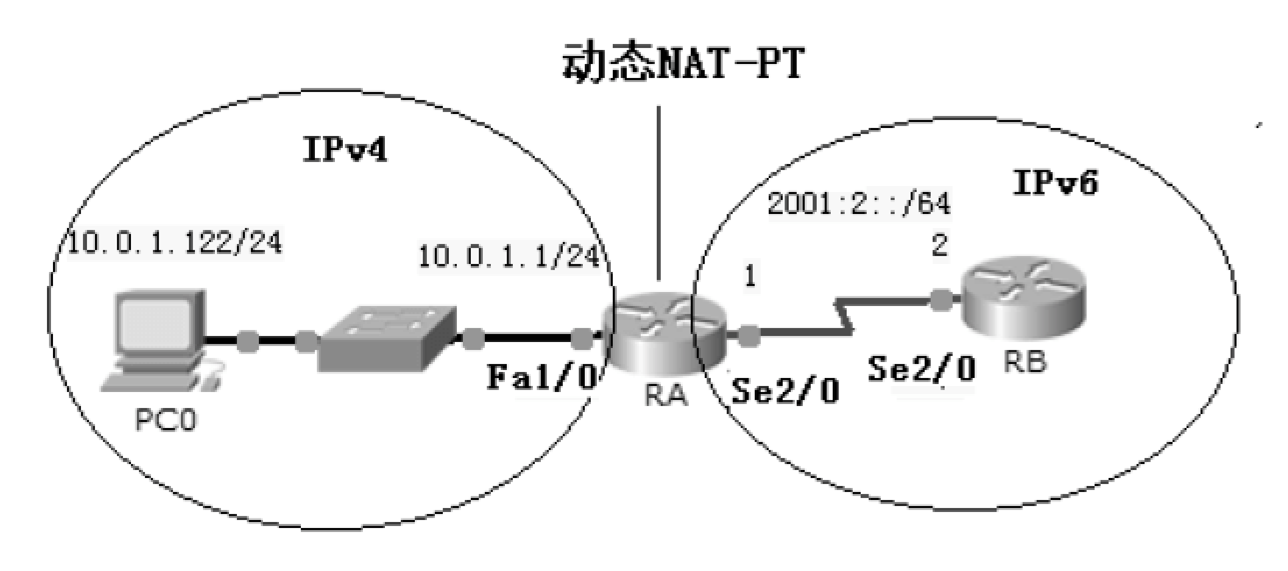
```
RB#debug ipv6 packet
IPv6 unicast packet debugging is on
RB#
*Mar  1 00:15:10.563: IPV6: source 2001:3::122 (Serial2/0)
*Mar  1 00:15:10.567:       dest 2001:2::2
*Mar  1 00:15:10.567:       traffic class 0, flow 0x0, len 88+4, prot 44, hops 1
27, forward to ulp
*Mar  1 00:15:10.571: IPv6: nexthop 2001:2::1,
*Mar  1 00:15:10.571: IPV6: source 2001:2::2 (local)
*Mar  1 00:15:10.575:       dest 2001:3::122 (Serial2/0)
*Mar  1 00:15:10.575:       traffic class 0, flow 0x0, len 80+4, prot 58, hops 6
4, originating
*Mar  1 00:15:10.579: IPv6: Sending on Serial2/0
*Mar  1 00:15:11.483: IPV6: source 2001:3::122 (Serial2/0)
*Mar  1 00:15:11.483:       dest 2001:2::2
*Mar  1 00:15:11.487:       traffic class 0, flow 0x0, len 88+4, prot 44, hops 1
27, forward to ulp
```

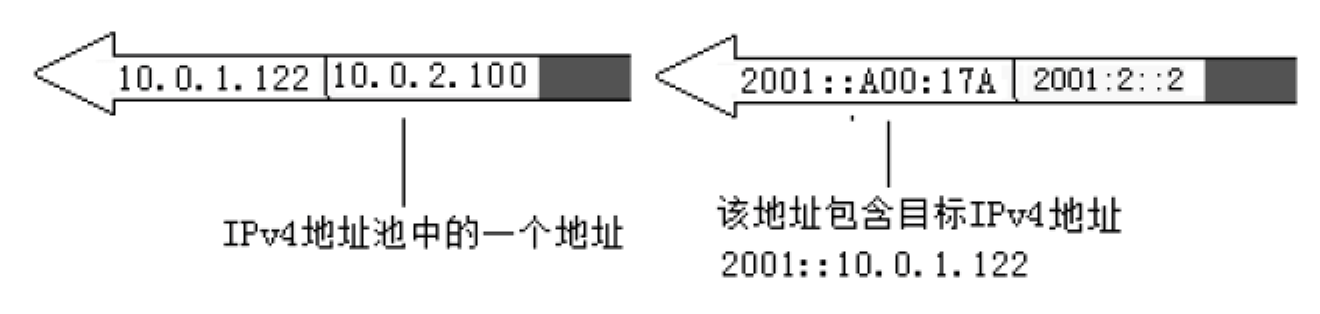
▲图 10-26　显示 IPv6 数据包

2. 示例：配置动态 NAT-PT

动态 NAT-PT 实验环境如图 10-27 所示，使 IPv6 网络 2001:2::/64 的计算机能够访问 IPv4 网络中的计算机。路由器 RB 需要访问 PC0 时，目标 IPv6 地址中包括 IPv4 地址，10.0.1.122 写成十六进制就是 A00:17A。

需要定义一个 IPv4 的地址池 10.0.2.100 ～ 10.0.2.200，这样只允许 101 个 IPv6 主机同时访问 IPv4 网络中的计算机。





▲图 10-27　动态 NAT-PT 实验环境

需要创建一个 IPv6 访问控制列表，指定允许哪些 IPv6 访问 IPv4 网络。

指定将 IPv4 的地址映射到 2001::/64 IPv6 网段。

动态 NAT-PT 实验步骤如下。

（1）在 RA 上配置动态 NAT-PT。

```
RA（config）#ipv6 unicast-routing
RA（config）#interface fastEthernet 1/0
RA （config-if）#ip address 10.0.1.1 255.255.255.0
RA （config-if）#no shutdown
RA（config-if）#ipv6 NAT
RA（config-if）#exit
RA（config）#interface Serial 2/0
RA（config-if）#clock rate 64000
RA（config-if）#no shutdown
RA（config-if）#ipv6 address 2001:2::1/64
RA（config-if）#ipv6 NAT
RA（config-if）#exit
RA（config）#ipv6 access-list v4map permit 2001:2::/64 any
RA（config）#ipv6 access-list v6list permit 2001:2::/64 any
RA（config）#ipv6 NAT prefix 2001::/96 v4-mapped v4map
RA（config）#ipv6 NAT v6v4 pool v4pool 10.0.2.100 10.0.2.200 prefix-length 24
RA（config）#ipv6 NAT v6v4 source list v6list pool v4pool
RA（config）#exit
RA#debug ipv6 NAT
```

（2）在路由器 RB 上添加 IPv6 地址和默认路由的步骤省略，在路由器 RB 上 ping PC0，该地址包含 IPv4 地址，PC0 的 IPv4 地址写成十六进制就是 A00:17A。

Ping 2001::A00:17A

（3）如图 10-28 所示是在路由器 RA 上的输出，可以看到源地址 2001:2::2 被 10.0.2.100 替换，目标地址 A00:17A 被 10.0.1.122 替换。现在 10.0.2.100 就和 2001:2::2 做了临时的映射。现在你需要在 PC0 上通过访问 10.0.2.100 访问 2001:2::2。

```
RA#debug ipv6 nat
IPv6 NAT-PT debugging is on
RA#
*Mar  1 00:20:02.947: IPv6 NAT: icmp src (2001:2::2) -> (10.0.2.100), dst
:A00:17A) -> (10.0.1.122)
*Mar  1 00:20:02.951: IPv6 NAT:  src (10.0.1.122) -> (2001::A00:17A), dst
2.100) -> (2001:2::2)
*Mar  1 00:20:02.963: IPv6 NAT:  src (10.0.1.122) -> (2001::A00:17A), dst
2.100) -> (2001:2::2)
*Mar  1 00:20:02.967: IPv6 NAT: icmp src (2001:2::2) -> (10.0.2.100), dst
:A00:17A) -> (10.0.1.122)
```

▲图 10-28　IPv6 NAT 输出

（4）在 PC0 上就可以 ping 10.0.2.100，通过路由器 RA，将该数据包发送给 2001:2::2。

（5）如图 10-29 所示，在路由器 RB 上，运行 debug ipv6 packet 命令。当 PC0 ping 10.0.2.100 时就有输出。

```
RB#debug ipv6 packet
IPv6 unicast packet debugging is on
RB#
*Mar  1 00:28:49.787: IPV6: source 2001::A00:17A (Serial2/0)
*Mar  1 00:28:49.791:       dest 2001:2::2
*Mar  1 00:28:49.791:       traffic class 0, flow 0x0, len 88+4, prot 44,
*Mar  1 00:28:49.795: IPv6: nexthop 2001:2::1,
```

▲图 10-29　IPv6 数据包事件输出

10.5 习 题

1. IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为______（IP Next Generation），它是 Internet 工程任务组（IETF）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别就是 IP 地址的长度从 32 位升为_______位。
2. IPv6_______协议是确定邻居结点之间关系的一组消息和进程，是一组 ICMPv6（Internet Control Message Protocol for IPv6）消息，管理着邻居结点（即同一链路上的结点）的交互。
3. 邻居发现协议用高效的______和单播消息代替了______、ICMPv4 路由器发现（Router Discovery）和 ICMPv4 重定向（Redirect）消息，并提供了一系列其他功能。
4. 未来获得 IPv4 地址会越来越难，IPv4 地址已变成一种稀缺资源，而互联网仍然在高速发展，NAT 是一个重要的解决方案，但 NAT 存在一些弊端，如 NAT 破坏了 IP 的______模型、NAT 阻止了________、NAT 的效率。
5. IPv6 主要有三种地址：______________、____________和____________。
6. 单播只能进行一对一的传输，它只能识别一个接口，并将报文传输到此地址。但是，IPv6 单播地址的类型可有多种，包括__________、__________和_________。
7. IPv6 地址中的 64 位 IEEE eui-64 格式接口标识符（InterfaceID）用来标识链路上的一个唯一的接口。这个地址是从接口的_______________变化而来的。
8. IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置插入十六进制数________。为了确保这个从 MAC 地址得到的接口标识符是唯一的，还要将 U/L 位（从高位开始的第 7 位）设置为“1”。最后得到的这组数就作为 eui-64 格式的接口 ID。
9. ____________是 IPv6 进行地址自动配置时的一个过程。
10. IPv6 通过 IPv4 网络的隧道的类型有：_________、___________、__________。
11. IPv6 扩展报头包括，路由项、_______、________、________、逐跳选项、目的选项。
12. 下列选项中________是本地站点地址所用的地址前缀。

    A. 2001::/10

B. FE80::/10

C. FEC0::/10

D. 2002::/10

13. 构架在 IPv4 网络上的两个 IPv6 孤岛互联，一般会使用________技术解决。

A. ISATAP 隧道

B. 配置隧道

C. 双栈

D. GRE 隧道

14. IPv6 和 IPv4 中的 IPv6 主机互联通常使用________技术解决。

A. ISATAP 隧道

B. 配置隧道

C. GRE 隧道

D. NATPT

15. 建立配置隧道会用到________这些命令序列。

A. interface tunnel

B. tunnel source

C. tunnel destiNATion

D. tunnel mode ipv6ip

16. 关于链路本地地址，下面说法正确的是________。

A. 是一种单播受限地址，本地链路内使用

B. 格式前缀为 1111 1110 10

C. 链路本地地址可用于邻居发现，且总是自动配置的

D. 包含链路本地地址的包永远也不会被 IPv6 路由器转发

17. 关于本地站点地址，下面说法正确的是________。

A. 单播受限地址，限于站点内使用

B. 格式前缀为 1111 1110 11

C. 本地站点地址总是自动配置的

D. 相当于 172.16.0.0/12 和 192.168.0.0/16 等 IPv4 私用地址空间

18. 关于组播地址，下面说法正确的是_______。

A. IPv6 多点传送地址格式前缀为 1111 1111

B. 除前缀，多播地址还包括标志、范围域和组 ID 字段

C. 标志位 4 位，高三位保留，初始化成 0，第一位为 0，表示一个被 IANA 永久分配的组播地址，为 1 则表示一个临时的多点传送地址

D. 范围域 4 位，是一个多点传送范围域，用来限制组播的范围

19. 简要描述 PMTU 发现的工作过程。

20. 简述 IPv6 主机无状态地址配置的过程。

习题答案

1. IPng、128
2. 邻居发现
3. 组播、ARP
4. 端到端、端到端的网络安全
5. TLA 地址、NLA、SLA
6. 全球单播地址、链路本地地址、站点本地地址
7. MAC
8. FFFE
9. 无状态的自动配置
10. 6 to 4 隧道、ISATAP 隧道、NAT-PT
11. 分段、认证、安全封装
12. C
13. A
14. A
15. A、B、C、D
16. A、B、C、D
17. A、B、D
18. A、C、D
19. PMTU 发现的工作过程是：源端主机先使用自己的 MTU 值向目的主机发送报文，如果中间路由器给源端返回一个错误消息，则源端主机使用更小的 MTU 值来重新发送这个报文，如此反复，直到目的端主机收到这个报文，从而确定网络中两台主机之间能够处理的最大报文的大小。
20. A．生成链路本地地址

 B．发送多播邻接点请求报文

 C．是否收到回应

 D．是，停止地址自动配置

 D．否，初始化链路本地地址→发送路由器请求报文→收到路由器回应报文，进行设置→生成无状态地址前缀+接口 ID→发送多播邻接点请求报文→是否收到回应

 E．是，停止自动配置

 E．否，初始化无状态地址

第 11 章　广　域　网

本章为大家介绍广域网使用的协议，重点讲授广域网协议 HDLC、PPP 和帧中继协议，同时还会介绍 VPN 的配置、使用 Cisco 路由器配置为远程访问服务器、使用 Windows Server 2003 配置为远程访问服务器。

本章主要内容：

- 广域网与局域网的区别
- 广域网连接类型
- 典型的广域网封装协议
- 广域网协议 HDLC 的配置和应用场景
- PPP 协议的应用场景和配置
- 配置路由器广域网接口支持帧中继永久虚电路
- 虚拟专用网（VPN）
- 配置 Cisco 路由器作为 VPN 服务器
- 配置 Windows Server 2003 作为 VPN 服务器

11.1 广域网简介

现在对比介绍广域网和局域网，以下的介绍没有严格从这两个词的原始定义和原始意思来解释。当代技术使得这一定义变得不是很清晰。

- 局域网（Local Area Network，简称 LAN）是指在某一区域内由多台计算机互联成的计算机组。一般企业或机构自己购买设备，将物理位置较近的办公区的计算机使用网络设备连接起来，覆盖范围在几千米以内。局域网使用的网络设备有集线器或交换机，带宽为 10M、100M、1000M 几个标准，而使用无线连接的局域网带宽标准为 54M。
- 广域网（Wide Area Network，简称 WAN）是一种跨越大的、地域性的计算机网络的集合。由专业的 Internet 服务器提供商（ISP）网通或电信提供广域网连接。比如你公司需要将石家庄一个办事处的局域网和北京总公司的网络连接起来，你公司不会找施工队架设和维护石家庄到北京的网络线路。你只需租用网通或电信的线路即可。广域网的带宽由企业所付的费用决定，比如我们使用的 ADSL 就是租用网通或电信的服务，带宽有 1M、2M、4M。

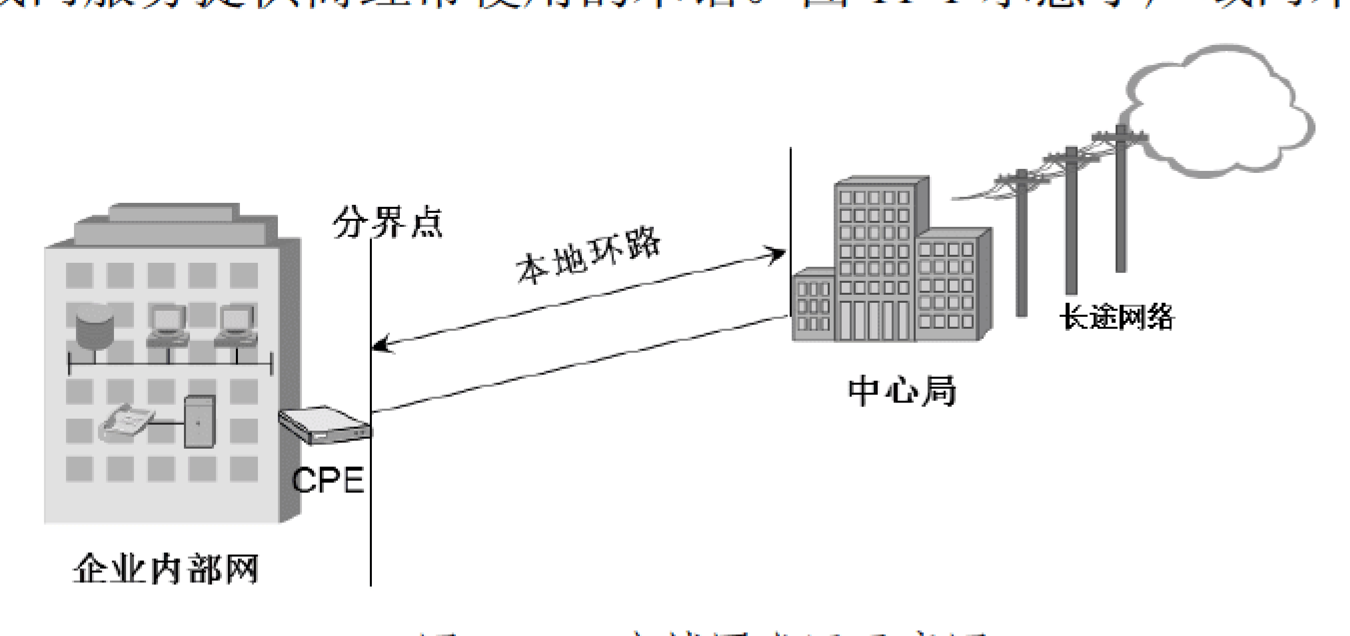
随着技术的发展，广域网和局域网的划分有时候也不是单纯从距离上划分的。比如你和邻居都分别使用 ADSL 访问 Internet，当你访问邻居的计算机共享文件或其他资源的时候，你的计算机和邻居的计算机就是广域网连接，因为你们是通过租用网通或电信提供的服务连接的；你和邻居的计算机如果使用网线直接连接，就是局域网连接。

再比如一个企业的两栋大楼距离几公里，这两栋大楼中的局域网通过公司的光纤连接，我们也可以将其理解为局域网，因为没有租用网通或电信提供的广域网链路，也就是没有使用广域网技术。

简而言之，局域网就是自己花钱购买网络设备，自己维护网络，带宽 10M、100M、1000M；广域网就是花钱租用广域网线路，网通或电信等 ISP 负责保证网络的连通性，带宽由费用决定。

11.1.1 广域网术语

下面介绍广域网服务提供商经常使用的术语。图 11-1 示意了广域网术语所指的概念。



▲图 11-1 广域网术语示意图

- 用户驻地设备（Customer Premises Equipment，CPE）：是用户方拥有的设备，位于用户驻地一侧。
- 分界点（Demarcation Point）：是服务提供商最后负责点，也是 CPE 的开始。通常是最靠近电信的设备，并且由电信公司拥有和安装。客户负责从此盒子到 CPE 的布线（扩展分界），通常是连接到 CSU/DSU 或 ISDN 接口。
- 本地环路（Local Looop）：连接分界点到称为中心局的最近交换局。
- 中心局（Central Office，CO）：这个点连接用户到提供商的交换网络，有时也指呈现点（POP）。
- 长途网络（Toll Network）：这些是广域网提供商网络中的中继线路。它是属于 ISP 的交换机和设备的集合。

熟悉这些术语非常重要，因为这是理解广域网技术的关键。

11.1.2 广域网连接类型

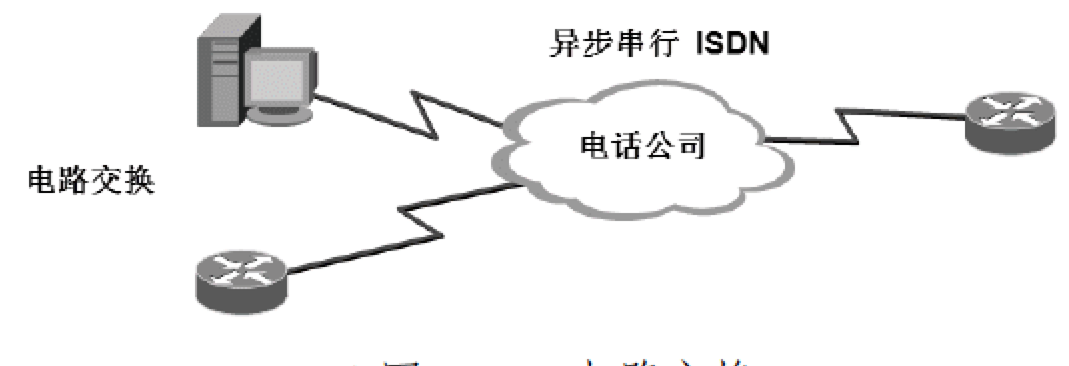
广域网可以使用许多不同的连接类型，这部分将介绍目前市场上常见的各种广域网连接类型。可以通过 DCE 网络将局域网连接在一起。下面解释广域网连接类型。

- 租用线路（Leased Lines）：租用线路典型地指点到点连接或专线连接，它是从本地 CPE 经过 DCE 交换机到远程 CPE 的一条预先建立的广域网通信路径。允许 DTE 网络在任何时候不用设置就可以传输数据进行通信。当不考虑使用成本时，它是最好的选择类型。它使用同步串行线路，速率最高可达 45Mb/s。租用线路通常使用 HDLC 和 PPP 封装类型，下面将会讲到这两种封装类型。租用线路适用于大数据传输，数据流量恒定的环境。一般建议在连接时间长、距离较短的场合使用，如图 11-2 所示。



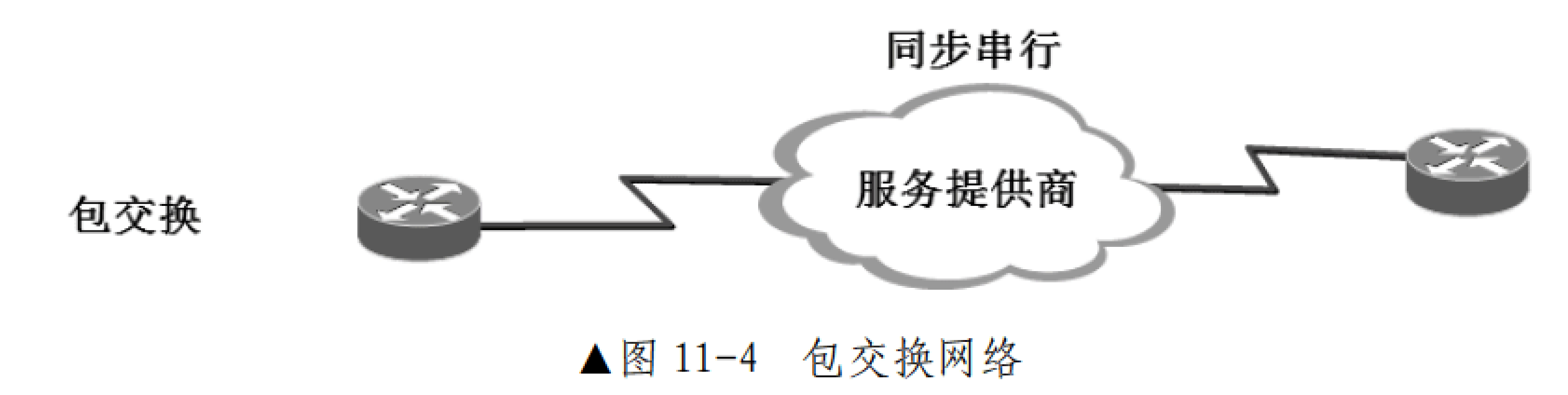
▲图 11-2　租用线路

- 电路交换（Circuit Switching）：当你听到电路交换这个术语时，就想一想电话呼叫。它最大的优势是成本低——只需为真正占用的时间付费。在建立端到端连接之前，不能传输数据。一般用在电话公司网络中，与我们日常拨打电话类似，是一种按需拨号技术，连接时使用专用物理线路，也用于备份连接、场点规模小、短时间的访问。常用的连接方式有：拨号上网、ISDN 和 ADSL，如图 11-3 所示。



▲图 11-3　电路交换

- 包交换（Packet Switching）：这是一种广域网交换方法，允许和其他公司共享带宽以节省资金。可以将包交换想像为一种看起来像租用线路，但费用更像电路交换的一种网络。不利因素是，如果需要经常传输数据，则不要考虑这种类型，应当使用租用线路；如果是偶然的突发性的数据传输，那么包交换可以满足需要。帧中继和 X.25 是包交换技术，速率从 56kb/s 到 T3（45Mb/s）。由于共享物理线路；包交换连接的性价比较高，一般可用于长时间连接或大地域跨度连接，如图 11-4 所示。



▲图 11-4　包交换网络

11.1.3　通用的广域网协议

如图 11-5 所示，Cisco 支持 HDLC、PPP 和帧中继。在任何串行接口执行 encapsulation ? 命令可以证实这一点（输出结果根据所运行 IOS 版本的不同而不同）。

```
RA(config)#interface serial 1/0
RA(config-if)#encapsulation ?
  atm-dxi          ATM-DXI encapsulation
  bstun            Block Serial tunneling (BSTUN)
  frame-relay      Frame Relay networks
  hdlc             Serial HDLC synchronous
  lapb             LAPB (X.25 Level 2)
  ppp              Point-to-Point protocol
  sdlc             SDLC
  sdlc-primary     SDLC (primary)
  sdlc-secondary   SDLC (secondary)
  smds             Switched Megabit Data Service (SMDS)
  stun             Serial tunneling (STUN)
  x25              X.25
```

▲图 11-5　路由器支持的广域网封装

如果路由器上有其他类型的接口，那么可以封装成其他类型，如 ISDN 或 ADSL。记住，不能在串行接口上配置以太网或令牌环网封装。

在这部分，我们将定义使用最突出的广域网协议——帧中继、ISDN、LAPD、 HDLC、PPP、 PPPoE、Cable、DSL、MPLS 和 ATM。但目前通常在串行接口上配置的广域网协议只有 HDLC、 PPP 和帧中继。

当前广大网民访问 Internet 使用最多的接入方式是 ADSL 接入，通过现有的电话线路作为 Internet 的接入线路，使用的协议为 PPPoE。

- ADSL 同时支持语音和数据的传输，它为下行流分配更多的带宽。家庭用户通常执行的操作（如下载视频、电影和音乐，在线游戏，网上冲浪和查看 E-mail，下载较大的附件）都需要更大的下行流带宽。ADSL 的下载速度在 256kb/s～8Mb/s 之间，但上传速度只能达到 1Mb/s。

- PPPOE（以太网上的点到点协议）和 ADSL 服务一起使用，它将 PPP 帧封装成以太帧，并使用 PPP 的一些如认证、封装和压缩等常用特征。但如前所述，防火墙配置差会很麻烦。有一个隧道协议可以将 IP 协议和其他协议分层，根据 PPP 链接的特性运行 PPP 协议，从而连接上其他的以太网设备并初始化点到点连接来传输 IP 包。

11.2 典型的广域网协议

Cisco 串行连接几乎支持广域网服务的任何类型。典型的广域网连接是使用 HDLC、PPP 和帧中继的专线，其速度可高达 45Mb/s（T3）。HDLC、PPP 和帧中继可以使用相同的物理层规范。

11.2.1 HDLC

HDLC，高级数据链路控制协议（High-Level Data-Link Control Protocol）是流行的 ISO 标准的、面向位的数据链路层协议。它使用帧特性、校验和规定数据在同步串行数据链路上的封装方法。HDLC 是一种用于租用线路的点到点协议。没有任何认证可以用于 HDLC。

在面向字节的协议中，用整个字节对控制信息进行编码；另一方面，面向位的协议可能使用单个位代表控制信息（面向位的协议包括 SDLC、LLC、HDLC、TCP、IP 等）。

HDLC 是 Cisco 路由器在同步串行线路上的默认封装方式。Cisco 的 HDLC 是专用的——不能和其他厂商的 HDLC 通信。但是不要为此抱怨 Cisco，每个厂商的 HDLC 都是专用的。图 11-6 显示了 Cisco 的 HDLC 格式。

每个厂商都有一种专用的 HDLC 封装方式的原因是，每个厂商解决 HDLC 和网络层协议通信时采用了不同的方法。如果厂商没有办法解决 HDLC 和不同的第 3 层协议的通信问题，那么 HDLC 只能携带一种协议。这个标识协议属性的报头位于 HDLC 封装的数据字段中。

如果你只有一台 Cisco 路由器，需要连接到一台非 Cisco 的路由器（因为另一台 Cisco 路由器正在订购中），该怎么办呢？不能使用默认的 HDLC 串行封装，因为它不能正常运行。你应当使用像 PPP 这样的能识别上层协议的 ISO 标准的封装方式。

Cisco HDLC

标志	地址	控制	专用	数据	帧校验序列（FCS）	标志

* 每个厂商的HDLC都有一个专用的数据字段以支持协议环境

HDLC

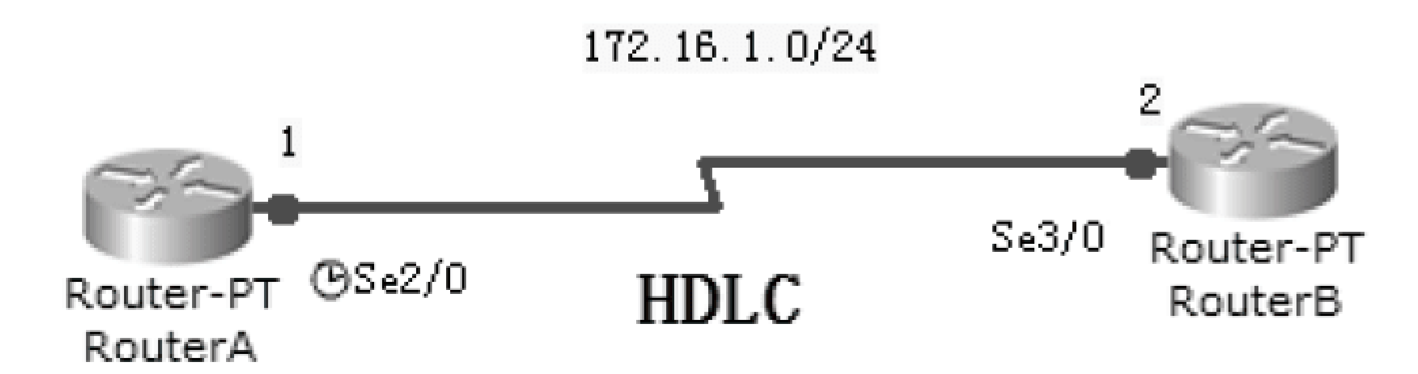
标志	地址	控制	数据	帧校验序列（FCS）	标志

* 只支持一个协议环境

▲图 11-6　HDLC 格式

配置广域网接口使用 HDLC 封装

打开随书光盘中第 11 章练习“01 配置广域网接口使用 HDLC 封装.pkt”，网络拓扑如图 11-7 所示。RouterA 和 RouterB 之间使用串口连接，你需要配置广域网链路使用 HDLC 封装。



▲图 11-7 配置 HDLC 封装

（1）配置 RouterA 广域网接口 Serial 2/0 使用 HDLC 封装。

```
RouterA>en
RouterA#config t
RouteA (config)#interface Serial 2/0
RouterA (config-if)#clock rate 64000
RouterA (config-if)#no sh
RouterA (config-if)#ip address 172.16.1.1 255.255.255.0
RouterA (config-if)#encapsulation ?        --查看广域网接口支持的封装类型
  frame-relay  Frame Relay networks
  hdlc         Serial HDLC synchronous
  ppp          Point-to-Point protocol
RouterA (config-if)#encapsulation hdlc     --配置接口使用 HDLC 封装
```

真正的路由器支持广域网封装类型的很多，但 Packet Tracer 模拟的路由器只支持这三种。

（2）在 RouterB 广域网接口 Serial 3/0 使用 HDLC 封装。

```
RouterB(config)#
RouterB(config)#interface Serial 3/0
RouterB(config-if)#ip address 172.16.1.2 255.255.255.0
RouterB(config-if)#encapsulation hdlc
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#exit
RouterB#show interfaces Serial 3/0
Serial3/0 is up,line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.16.1.2/24
```

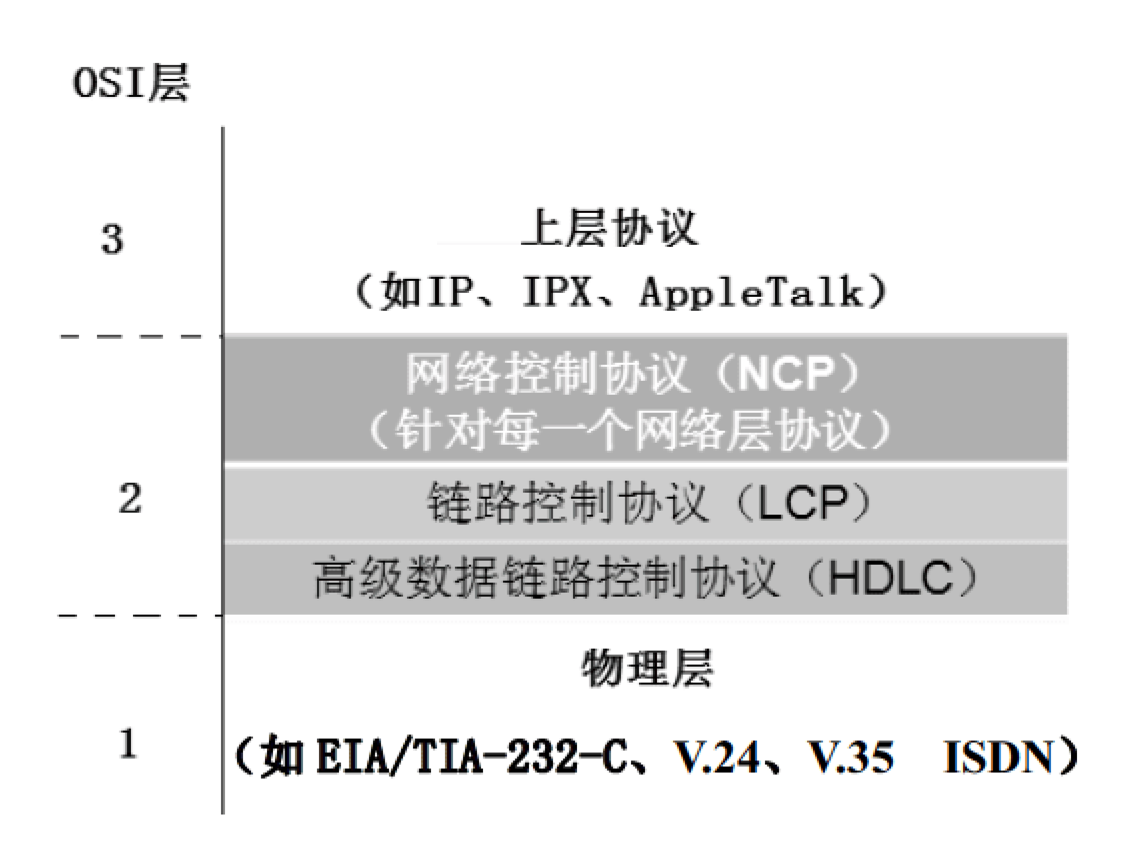
```
MTU 1500 bytes,BW 128 Kbit,DLY 20000 usec
   reliability 255/255,txload 1/255,rxload 1/255
Encapsulation HDLC,loopback not set,keepalive set （10 sec）
```

其中，第一个 up 代表物理接口 up，第二个 up 代表数据链路层 up。如果广域网接口两端封装不一致，则会出现 Serial3/0 is up,line protocol is down （connected）。可以看到封装类型为 HDLC。

11.2.2 点到点 PPP

PPP（Point-To-Point Protocol，点到点协议）可以用于异步串行（拨号）或同步串行（ISDN）介质。它使用 LCP（Link Control Protocol，链路控制协议）建立并维护数据链路连接。NCP（Network Control Protocol，网络控制协议）允许在点到点连接上使用多种网络层协议（被动路由协议），如图 11-8 所示。

既然 HDLC 是 Cisco 串行链路上默认的串行封装协议，并且 HDLC 的性能非常好，那么什么时候使用 PPP 呢？PPP 的基本目标是在数据链路层点到点链路上传输第 3 层包。它不是一个专用协议，这意味着如果你的路由器并不都是 Cisco 的，在串行接口上就需要封装 PPP，由于 HDLC 是 Cisco 专用协议，所以封装 HDLC 后不会正确运行。另外，既然 PPP 可以封装多种第 3 层被动路由协议，并且提供认证、动态寻址以及回叫功能，那么这些都是放弃 HDLC 而选择 PPP 作为封装方案的理由。



▲图 11-8　PPP 协议层次

PPP 包含的 4 个主要组件如下。

- EIA/TIA-232-C、V.24、V.35 和 ISDN 串行通信的物理层国际标准。
- 在串行链路上封装数据包的方法——HDLC。
- 建立、配置、维护和结束点到点连接的方法——LCP。
- 建立和配置不同网络层协议的方法——NCP。NCP 设计允许同时使用多个网络层协议。例如有些协议是 IPCP（Internet Protocol Control Protocol，因特网协议控制协议）和 IPXCP（Internetwork Packet Exchange Control Protocol，互联网络包交换控制协议）。

理解 PPP 协议栈只是物理层和数据链路层的规范非常重要。NCP 通过对 PPP 数据链路上的协议进行封装来允许在多种网络层协议之间实现通信。

提示	如果当一台 Cisco 路由器和一台非 Cisco 路由器通过串行连接在一起，必须配置 PPP 或另一种封装方法，像帧中继，因为默认的 HDLC 不能工作!

下面将讨论 LCP 和 PPP 会话的建立。

1）LCP 的配置选项

LCP 提供各种 PPP 封装选项，包括如下内容。

- Authentication（认证）：该选项告诉链路的呼叫方发送可以确定其用户身份的信息。两种方法是 PAP（Password Authentication Protcol，密码认证协议）和 CHAP（Challenge Handshke Authentication，问答握手认证协议）。
- Compression（压缩）：该选项用于通过传输之前压缩数据或负载来增加 PPP 连接的吞吐量。PPP 在接收端解压数据帧。
- Error Detection（错误检测）：PPP 使用 Quality（质量）和 Magic Number（魔术号码）选项确保可靠的、无环路的数据链路。
- Multilink（多链路）：从 IOS 11.1 版本开始，Cisco 路由器在 PPP 链路上支持多条链路选项。该选项允许几条不同的物理路径在第 3 层表现为一条逻辑路径。例如，运行 PPP 多链路的两条 T1 线路在第 3 层路由协议中以一条 3Mb/s 路径的形式出现。
- PPP callback（PPP 回叫）：PPP 可以配置为认证成功后进行回叫。PPP 回叫对于账户记录或各种其他原因是一个很好的功能，因为可以根据访问费用跟踪使用情况。启动回叫后，呼叫路由器（客户端）将和远程路由器（服务器端）取得联系，并像前面描述的那样进行认证。两台路由器必须都配置回叫。一旦完成认证，远程路由器将中断连接，并从远程路由器重新初始化到呼叫路由器的连接。

说明	如果在 PPP 回叫中使用的是 Microsoft 设备，要意识到 Microsoft 可能使用它专用的回叫功能，即微软回叫控制协议（Microsoft Callback Control Protocol，MCCP），并且 IOS 11.3 以上版本是支持这种回叫协议的。

2）PPP 会话的建立

当 PPP 连接开始时，链路经过以下 3 个会话建立阶段。

- 链路建立阶段：每台 PPP 设备发送 LCP 包来配置和测试链路。LCP 包包括一个叫“配置选项”的字段，允许每台设备查看数据的大小、压缩和认证。如果没有设置“配置选项”字段，则使用默认配置。
- 认证阶段：如果配置了认证，在认证链路时可以使用 CHAP 或 PAP。认证发生在读取网络层协议信息之前，同时可能发生链路质量决策。
- 网络层协议阶段：PPP 使用 NCP 协议，允许封装成多种网络层协议并在 PPP 数据链路上发送。每个网络层协议（例如 IP、IPX、AppleTalk 这些被动路由协议）都建立和 NCP 的服务关系。

3）PPP 认证方法

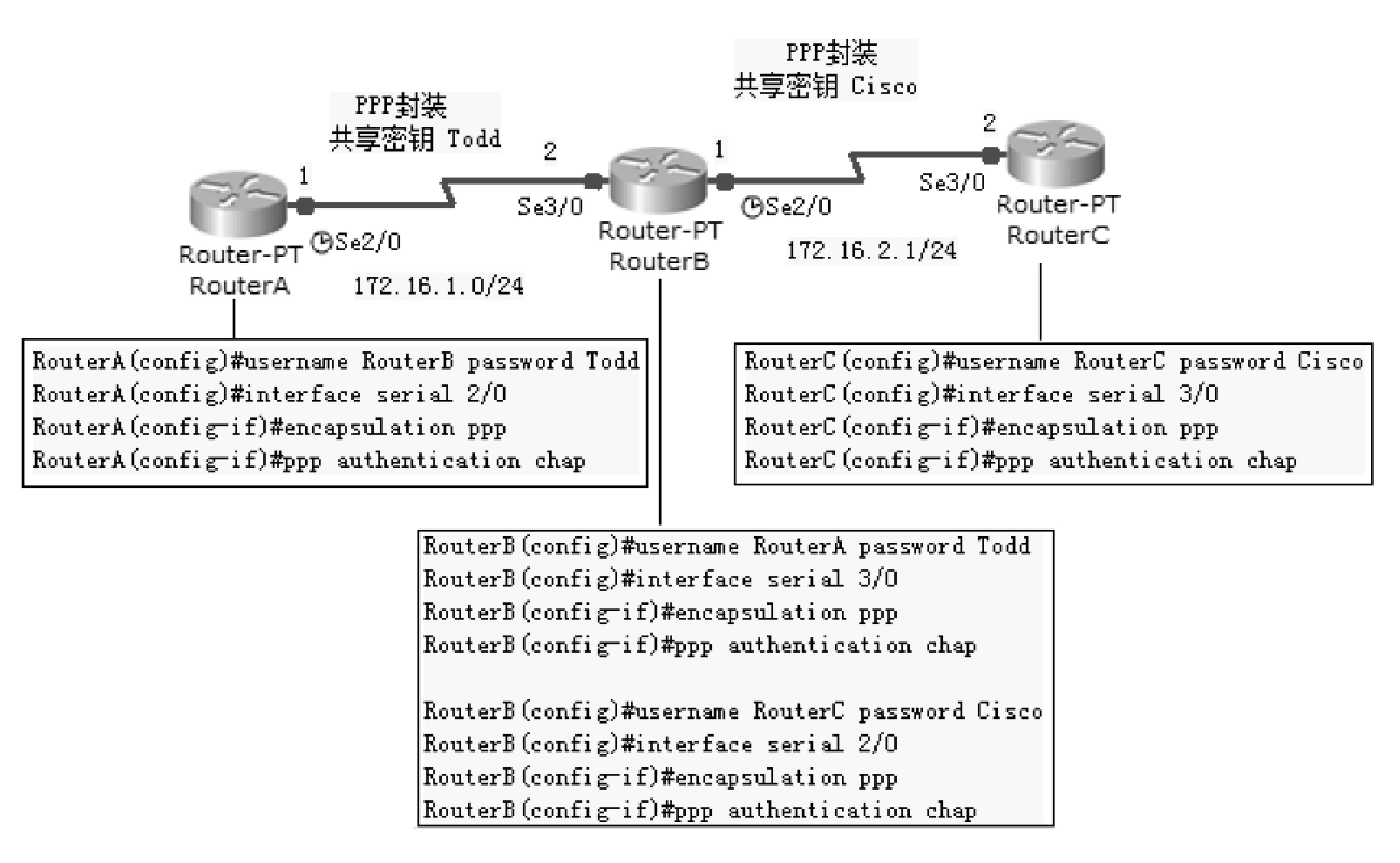
PPP 链路可以使用以下两种认证方法。

- PAP：PAP 是两种方法中安全程度较低的一种。口令以明文发送，并且 PAP 只在初始链路建立时执行。在 PPP 链路首次建立时，远程结点向发送路由器回送路由器用户名和口令，直到获得认证。
- CHAP：CHAP 用于链路初始启动，并且为了证实路由器连接的仍然是同一台主机，要进行周期性的链路检查。

PPP 结束了初始阶段后，本地路由器向远程设备发送一个盘问请求。远程设备发送一个用叫做 MD5 的单方向散列函数计算出来的值。本地路由器要检查此散列值，确定它是否匹配。如果这个值不匹配，该链路立即结束。

配置广域网接口使用 PPP 封装

打开随书光盘中第 11 章练习“02 配置广域网接口使用 PPP 封装.pkt”，网络拓扑如图 11-9 所示。你需要配置 RouterA 和 RouterB 之间的连接使用 PPP 封装，共享密钥为 Todd，配置 RouterB 和 RouterC 之间的连接使用 PPP 封装，共享密钥为 Cisco，PPP 认证方法为 CHAP，并且诊断 PPP 认证的过程。



▲图 11-9 配置 PPP 封装

（1）在 RouterA 上配置和 RouterB 连接的 PPP 封装和共享密钥。

```
RouterA (config) #interface Serial 2/0
RouterA (config-if) #clock rate 64000
RouterA (config-if) #ip address 172.16.1.1 255.255.255.0
RouterA (config-if) #no sh
```

```
RouterA(config-if)#encapsulation ppp      --配置使用 PPP 封装
RouterA(config-if)#ppp authentication ?  --查看支持的认证方法
  chap  Challenge Handshake Authentication Protocol <CHAP>
  pap   Password Authentication Protocol <PAP>
RouterA(config-if)#ppp authentication chap
RouterA(config-if)#ex
RouterA(config)#username RouterB password Todd
                                       --配置和 RouterB 路由器的共享密钥
```

（2）在 RouterB 上查看串口默认的数据封装类型和接口状态。

```
RouterB(config)#interface Serial 3/0
RouterB(config-if)#ip address 172.16.1.2 255.255.255.0
RouterB(config-if)#no sh
RouterB(config-if)#^Z
RouterB #show interfaces Serial 3/0
Serial3/0 is up,line protocol is down (disabled)
                                       --协议 down，两端封装不一致
  Hardware is HD64570
  Internet address is 172.16.1.2/24
  MTU 1500 bytes,BW 128 Kbit,DLY 20000 usec,
     reliability 255/255,txload 1/255,rxload 1/255
  Encapsulation HDLC,loopback not set,keepalive set (10 sec)
                                       --默认为 HDLC 封装
```

（3）在 RouterB 上配置和 RouterA 连接的封装类型为 PPP。

```
RouterB(config)#interface Serial 3/0
RouterB(config-if)#encapsulation ppp  --配置为 PPP 封装
RouterB(config-if)#^Z                 --按 Ctrl + C 组合键，退回到特权模式
```

（4）在 RouterB 上查看和 RouterA 连接 PPP 协议的状态。

```
RouterB#show interfaces Serial 3/0
Serial3/0 is up,line protocol is down (disabled)
  Hardware is HD64570
  Internet address is 172.16.1.2/24
  MTU 1500 bytes,BW 128 Kbit,DLY 20000 usec,
     reliability 255/255,txload 1/255,rxload 1/255
  Encapsulation PPP,loopback not set,keepalive set (10 sec)--PPP 封装
  LCP Closed          --链路控制协议关闭，没有配置和 RouterA 的共享密码
  Closed: LEXCP,BRIDGECP,IPCP,CCP,CDPCP,LLC2,BACP  --网络层协议均关闭
```

（5）在 RouterB 上配置和 RouterA 的共享密码。

```
RouterB（config）#username RouterA password Todd
                                              --配置和 RouterA 的共享密码
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0,changed state
to up 接口状态变为 up
```

（6）在 RouterB 上查看和 RouterA 连接的端口状态。

```
RouterB#show interfaces Serial 3/0
Serial 3/0 is up,line protocol is up （connected） --数据链路层 up
  Hardware is HD64570
  Internet address is 172.16.1.2/24
  MTU 1500 bytes,BW 128 Kbit,DLY 20000 usec,
     reliability 255/255,txload 1/255,rxload 1/255
  Encapsulation PPP,loopback not set,keepalive set （10 sec）
  LCP Open              --链路控制协议打开
  Open: IPCP,CDPCP      --支持的网络层协议打开
```

（7）在 RouterB 上配置和 RouterC 共享的密码和封装类型。

```
RouterB（config）#interface Serial 2/0
RouterB（config-if）#clock rate 64000
RouterB（config-if）#no sh
RouterB（config-if）#ip address 172.16.2.1 255.255.255.0
RouterB（config-if）#encapsulation ppp
RouterB（config-if）#ppp authentication chap
RouterB（config-if）#ex
RouterB（config）#username RouterC password Cisco
```

（8）在 RouterC 上配置和 RouterB 的共享密码和封装类型。

```
RouterC（config）#interface Serial 3/0
RouterC（config-if）#ip address 172.16.2.2 255.255.255.0
RouterC（config-if）#no sh
RouterC（config-if）#encapsulation ppp
RouterC（config-if）#ppp authentication chap
RouterC（config-if）#ex
RouterC（config）#username RouterB password Cisco
```

（9）在 RouterA 上诊断 PPP 认证。

```
RouterA#debug ppp authentication
RouterA#config t
RouterA（config）#interface Serial 2/0
```

```
RouterA（config-if）#shutdown            --禁用接口
RouterA（config-if）#no shutdown         --启用接口，可以看到 PPP 验证的过程
%LINK-5-CHANGED: Interface Serial 2/0,changed state to up
Serial 2/0 IPCP: I CONFREQ [Closed] id 1 len 10
Serial 2/0 IPCP: O CONFACK [Closed] id 1 len 10
Serial 2/0 IPCP: I CONFREQ [REQsent] id 1 len 10
Serial 2/0 IPCP: O CONFACK [REQsent] id 1 len 10
```

11.2.3 帧中继

帧中继已成为近几十年广域网服务最流行的技术之一。它有很多受欢迎的原因，但主要是由于费用较低。帧中继比其他技术更节省费用，这是网络设计不可忽略的因素。

1．帧中继简介

帧中继默认情况下属于非广播多路访问（None Broadcast MultiAccess ，NBMA）网络，意思是默认情况下不在网络上发送像 RIP 更新这样的广播包。将在后面进一步讨论这个特性。

帧中继是从 X.25 技术发展来的。考虑到目前可靠性和比较“清洁”的电信网络，帧中继本质上和 X.25 的功能是不相容的，忽略了不再需要的纠错功能。它和在 HDLC 和 PPP 协议中学到的简单租用线路网络相比显得非常复杂。这些租用线路是易于构建的，帧中继却不是。它可能非常复杂和多变，这就是为什么在网络图形中经常用“网云”代表它的原因。后面将会介绍它。这里将从概念上介绍帧中继，并介绍如何区别它和简单的租用线路技术。

在 CCNA 考试中，要求你理解帧中继技术的基本原理，并能够在简单的场景中进行配置。首先理解帧中继是包交换技术。从目前学到的知识来看，只告诉你这一点应当使你想起和包交换有关的几件事情。

- 不能使用 encapsulation hdlc 或 encapsulation ppp 命令进行配置。
- 帧中继和点到点租用线路不一样（尽管可以做到，看起来像租用线路）。
- 帧中继在许多情况下没有租用线路昂贵，但是为了节省费用会有些损失。

1）数据链路连接标识符

帧中继 PVC 使用数据链路连接标识符（Data Link Connection Identity，DLCI）标识 DTE 设备。帧中继服务提供商分配 DLCI 值，帧中继用 DLCI 值区分网络上的不同虚电路。因为在一个多点帧中继接口上可以有多个虚电路，所以这种接口可以有多个 DLCI。

2）虚电路

帧中继使用虚电路工作方式，所谓“虚”是相对于租用线路使用的真正电路而言的。这些虚电路是由连接到提供商“网云”上的几千台设备构成的链路。帧中继为两台 DTE 设备

之间建立的虚电路，使它们就像通过一条电路连接起来一样，实际上是将帧放入一个很大的共享设施中。因为有了虚电路，你永远都不会看到“网云”内部所发生的复杂操作。

有两种虚电路——永久虚电路和交换虚电路。

永久虚电路（Permanent Virtual Circuits，PVC）是目前最常用的类型。永久的意思是电信公司在内部创建映射，并且只要你付费，虚电路就一直有效。

交换虚电路（Switch Virtual Circuits，SVC）更像电话呼叫。当数据需要传输时，建立虚电路；数据传输完成后，拆除虚电路。

3）子接口

正如前面讲过的，可能在一个串行接口上有多条虚电路，并且将每条虚电路视为一个单独的接口，它被认为是子接口。可以将子接口想象为一个由 IOS 软件定义的逻辑接口。多个子接口将共享一个物理硬件接口，但为了配置，把它们想象为单独的物理接口（称为复用）。

若想将帧中继网络中的路由器配置为避免水平分割阻止路由更新，可以为每条 PVC 配置多个子接口，并且为每个子接口分配唯一的 DLCI 和子网地址。

可以用 interface Se1/0.1 这样的命令定义子接口。首先必须在物理串行接口上设置封装类型，然后定义子接口。一般一个子接口定义一条 PVC。

点到点：当一条虚电路连接一台路由器到另一个路由时，使用点到点子接口。每个点到点子接口需要自己的子网。

多点：当路由器位于星状虚电路的中心时，使用多点子接口。所有连接到帧中继交换机上的路由器接口都使用同一个子网。

2．帧中继配置实例

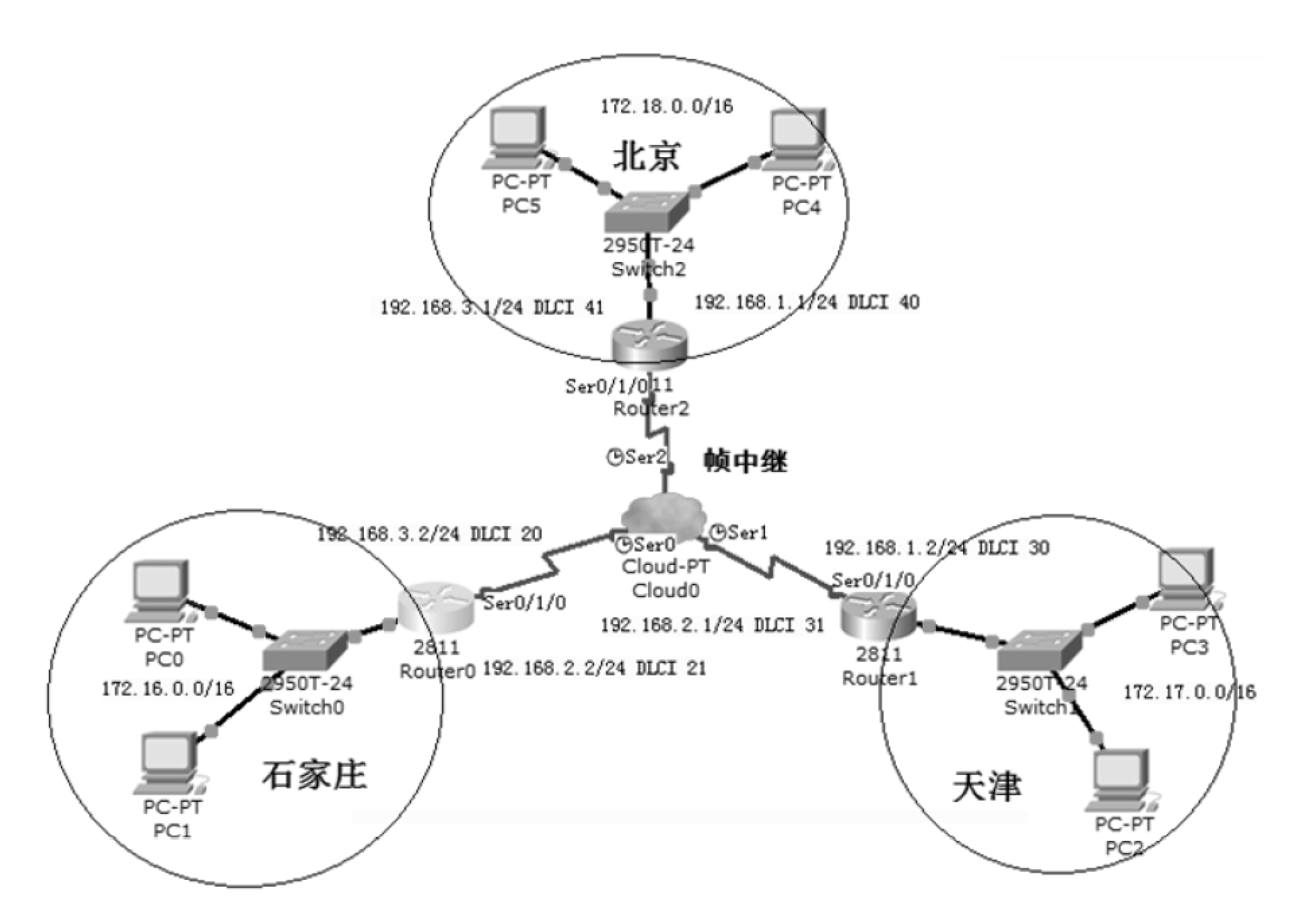
下面通过 Packet Tracer 软件搭建帧中继实验环境，为大家介绍使用帧中继连接多个局域网、配置路由器广域网接口使用帧中继封装，以及如何在一个路由器的物理接口配置子接口支持多条虚拟电路的过程。

打开随书光盘中第 11 章练习“03 帧中继配置实例.pkt”，网络拓扑如图 11-10 所示。某公司的总公司在北京，石家庄和天津有分公司，使用帧中继网络将 3 个城市的网络连接。现在需要你配置这些路由器和帧中继实现以下功能。

- 配置图 11-9 中的 3 个路由器使用帧中继连接。
- 逻辑上实现北京、石家庄和天津 3 个路由器全互联。
- 配置网络中的路由器使用 EIGRP 协议学习到各个网络的路由。
- 验证广域网配置。

1）物理连接拓扑

物理连接拓扑如图 11-10 所示。

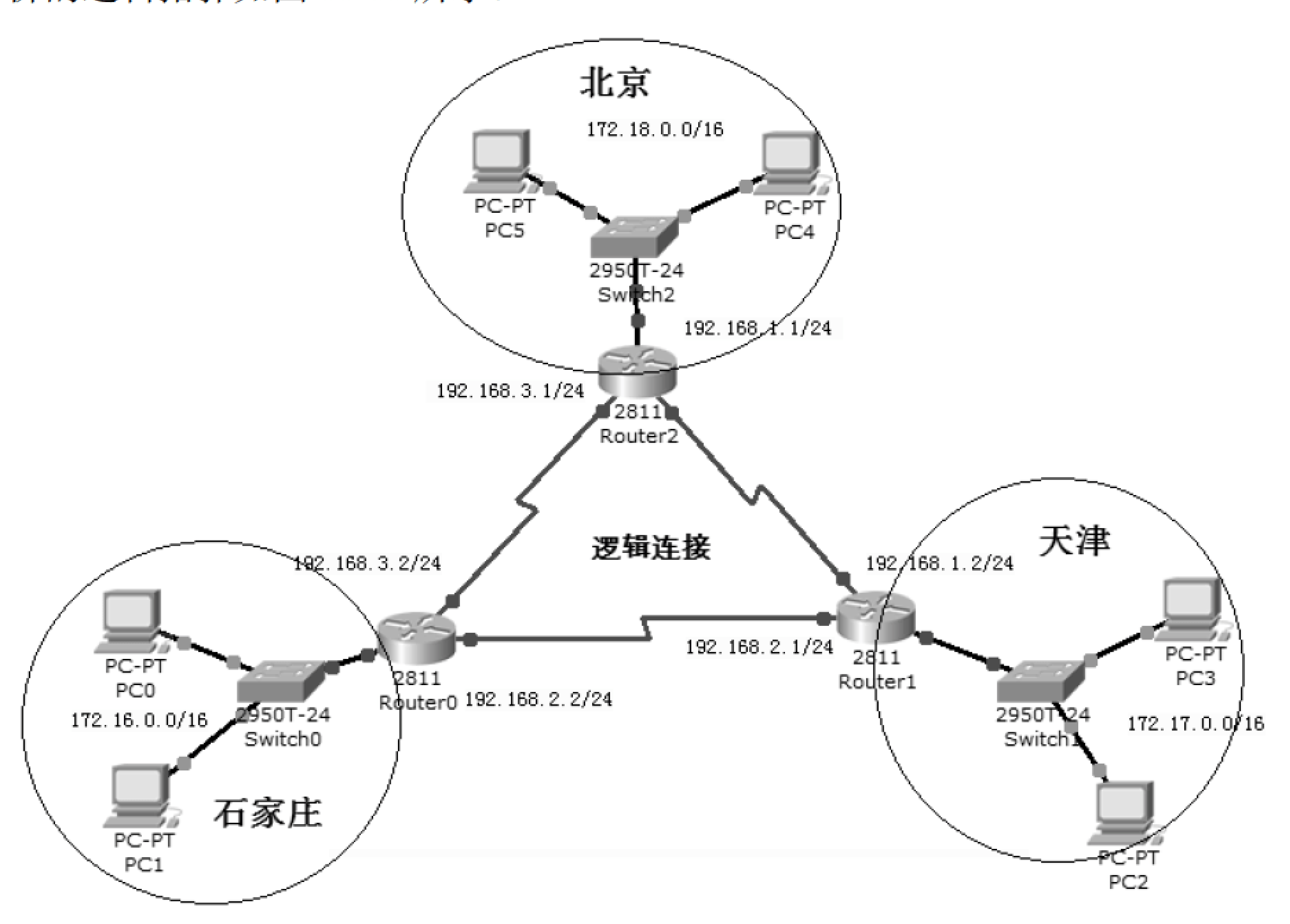


▲图 11-10 帧中继实验物理拓扑

通过将连接帧中继网络的路由器的串口配置为多个子接口，实现北京、石家庄和天津 3 个局域网全互联。

2）等价的逻辑连接

等价的逻辑拓扑如图 11-11 所示。



▲图 11-11 帧中继逻辑拓扑

3）配置步骤

（1）在 Router0 上，配置路由器广域网接口使用帧中继封装，并且配置子接口和对应的帧中继 DLCI，以及 EIGRP 动态路由协议。

```
    Router（config）#hostname Router0
    Router0（config）#interface Serial 0/1/0
    Router0（config-if）#encapsulation frame-relay
                                              --在物理接口配置封装帧中继
    Router0（config-if）#no sh                --启用物理接口，不要配置 IP 地址
    Router0（config-if）#ex
    Router0（config）#interface Serial 0/1/0.1 ? --进入子接口
     multipoint      Treat as a multipoint link
     point-to-point  Treat as a point-to-point link
     <cr>
    Router0（config）#interface Serial 0/1/0.1 point-to-point
                                              --配置逻辑子接口，点到点封装
    %LINK-5-CHANGED: Interface Serial0/1/0.1, changed state to up
    %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0.1, changed
state to up
    Router0（config-subif）#ip address 192.168.3.2 255.255.255.0
                                              --配置子接口 IP 地址
    Router0（config-subif）#description Link Router0 DLCI 20
                                              --配置描述，可选的配置
    Router0（config-subif）#frame-relay interface-dlci 20
                                              --数据链路连接标识符
    Router0（config-subif）#ex
    Router0（config）#interface serial 0/1/0.2 point-to-point
    Router0（config-subif）#ip address 192.168.2.2 255.255.255.0
    Router0（config-subif）#frame-relay interface-dlci 21
    Router0（config-subif）#exi
    Router0（config）#router eigrp 10          --配置路由协议
    Router0（config-router）#network 172.16.0.0
    Router0（config-router）#network 192.168.3.0
    Router0（config-router）#network 192.168.2.0
```

（2）在 Router1 上，配置路由器广域网接口使用帧中继封装，并且配置子接口和对应的帧中继 DLCI，以及 EIGRP 动态路由协议。

```
    Router （config）#hostname Router1
```

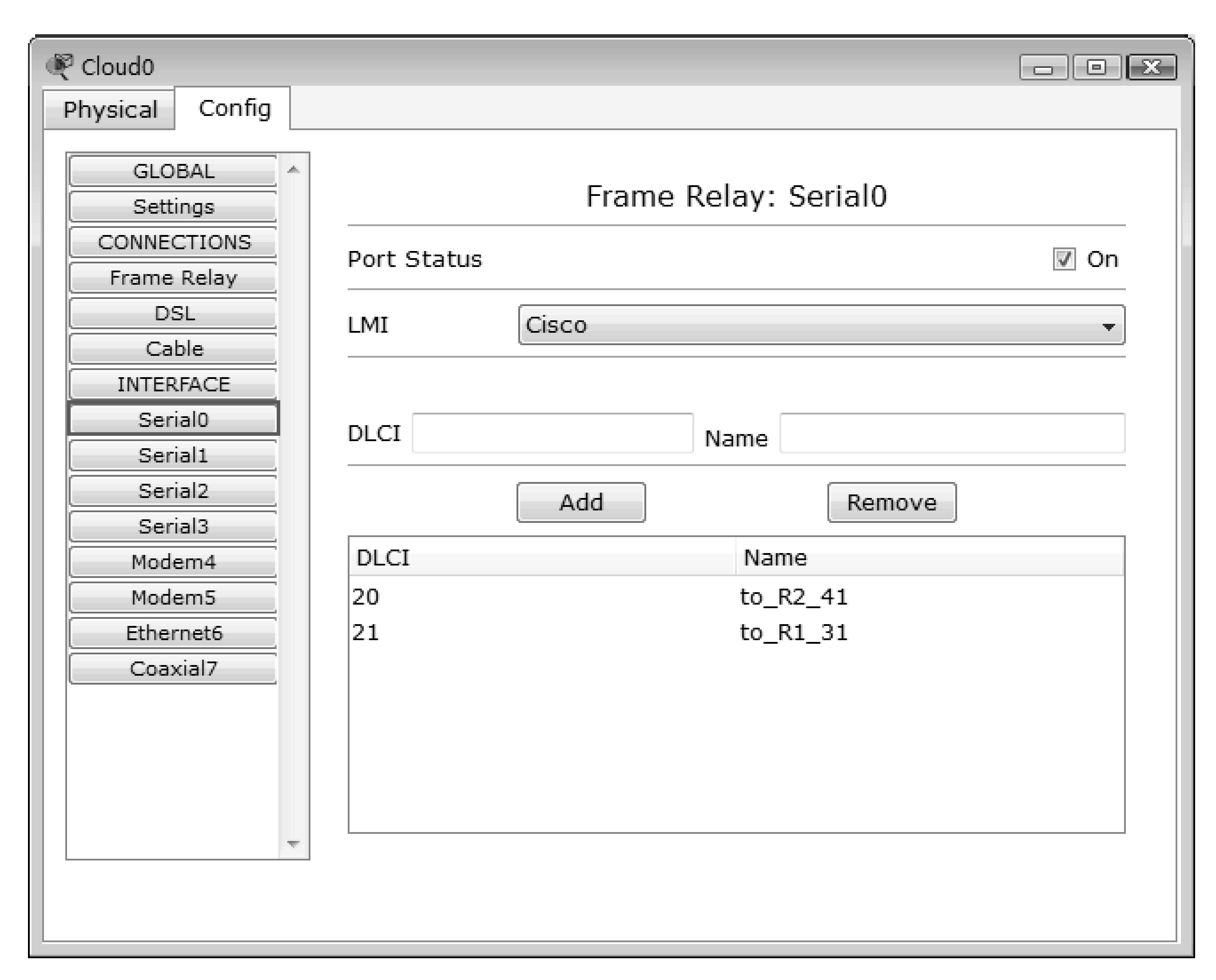
```
Router1 (config) #interface Serial 0/1/0
Router1 (config-if) #encapsulation frame-relay
Router1 (config-if) #no sh
Router1 (config-if) #exit
Router1 (config) #interface serial 0/1/0.1 point-to-point
Router1 (config-subif) #ip address 192.168.1.2 255.255.255.0
Router1 (config-subif) #frame-relay interface-dlci 30
Router1 (config-subif) #ex
Router1 (config) #interface serial 0/1/0.2 point-to-point
Router1 (config-subif) #ip address 192.168.2.1 255.255.255.0
Router1 (config-subif) #frame-relay interface-dlci 31
Router1 (config-subif) #ex
Router1 (config) #router eigrp 10
Router1 (config-router) #network 172.17.0.0
Router1 (config-router) #network 192.168.2.0
Router1 (config-router) #network 192.168.1.0
```

（3）在 Router2 上，配置路由器广域网接口使用帧中继封装，并且配置子接口和对应的帧中继 DLCI，以及 EIGRP 动态路由协议。

```
Router (config) #hostname Router2
Router2 (config) #interface Serial 0/1/0
Router2 (config-if) #no sh
Router2 (config-if) #encapsulation frame-relay
Router2 (config-if) #ex
Router2 (config) #interface serial 0/1/0.1 point-to-point
Router2 (config-subif) #ip address 192.168.1.1 255.255.255.0
Router2 (config-subif) #frame-relay interface-dlci 40
Router2 (config-subif) #exi
Router2 (config) #interface serial 0/1/0.2 point-to-point
Router2 (config-subif) #ip address 192.168.3.1 255.255.255.0
Router2 (config-subif) #frame-relay interface-dlci 41
Router2 (config-subif) #ex
Router2 (config) #router eigrp 10
Router2 (config-router) #network 172.18.0.0
Router2 (config-router) #network 192.168.3.0
Router2 (config-router) #network 192.168.1.0
```

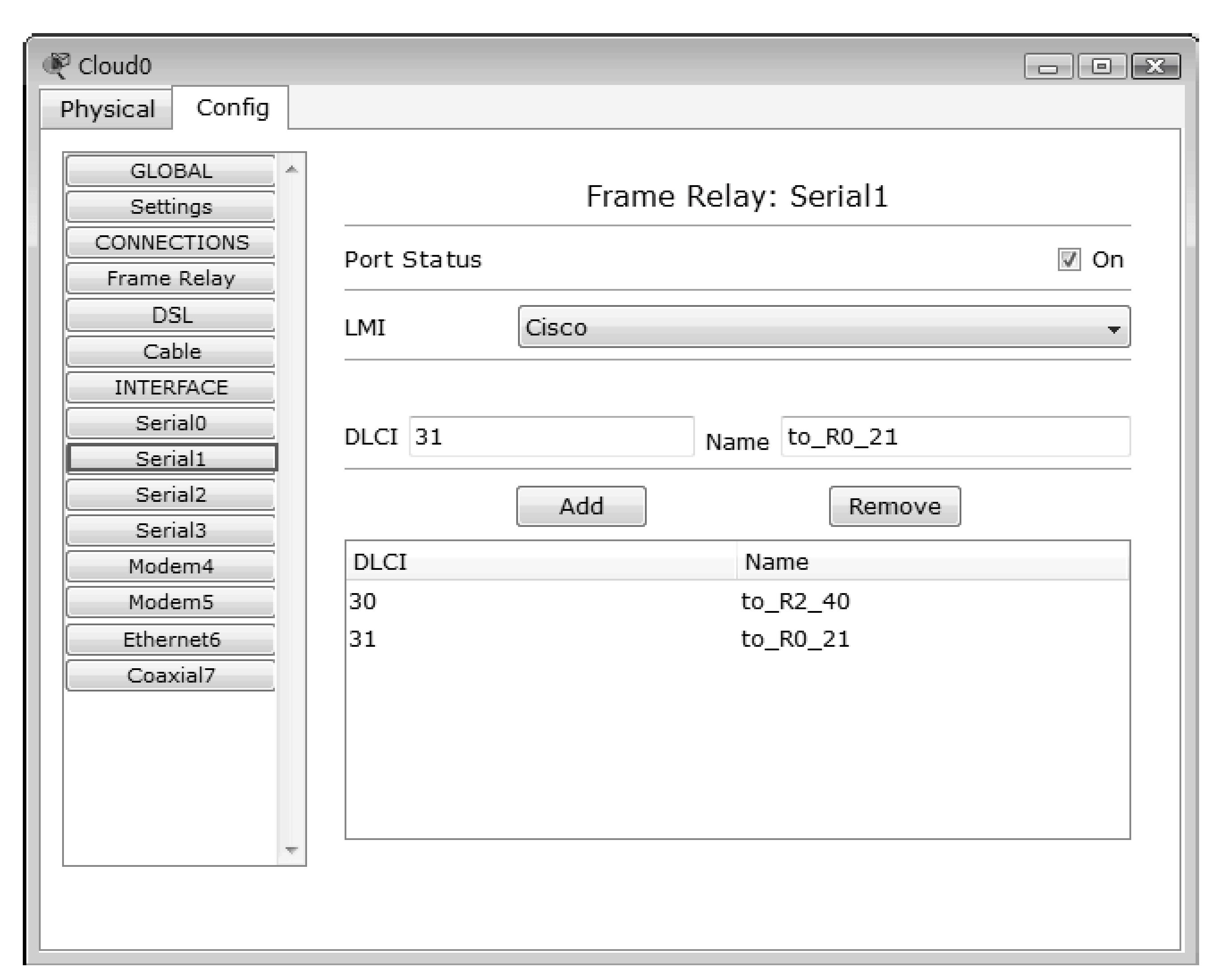
（4）如图 11-12 所示，配置帧中继接口的 DLCI。选中 Serial0，DLCI 输入 20，Name

输入 to_R2_41，单击 Add 按钮；DLCI 输入 21，Name 输入 to_R1_31，单击 Add 按钮。



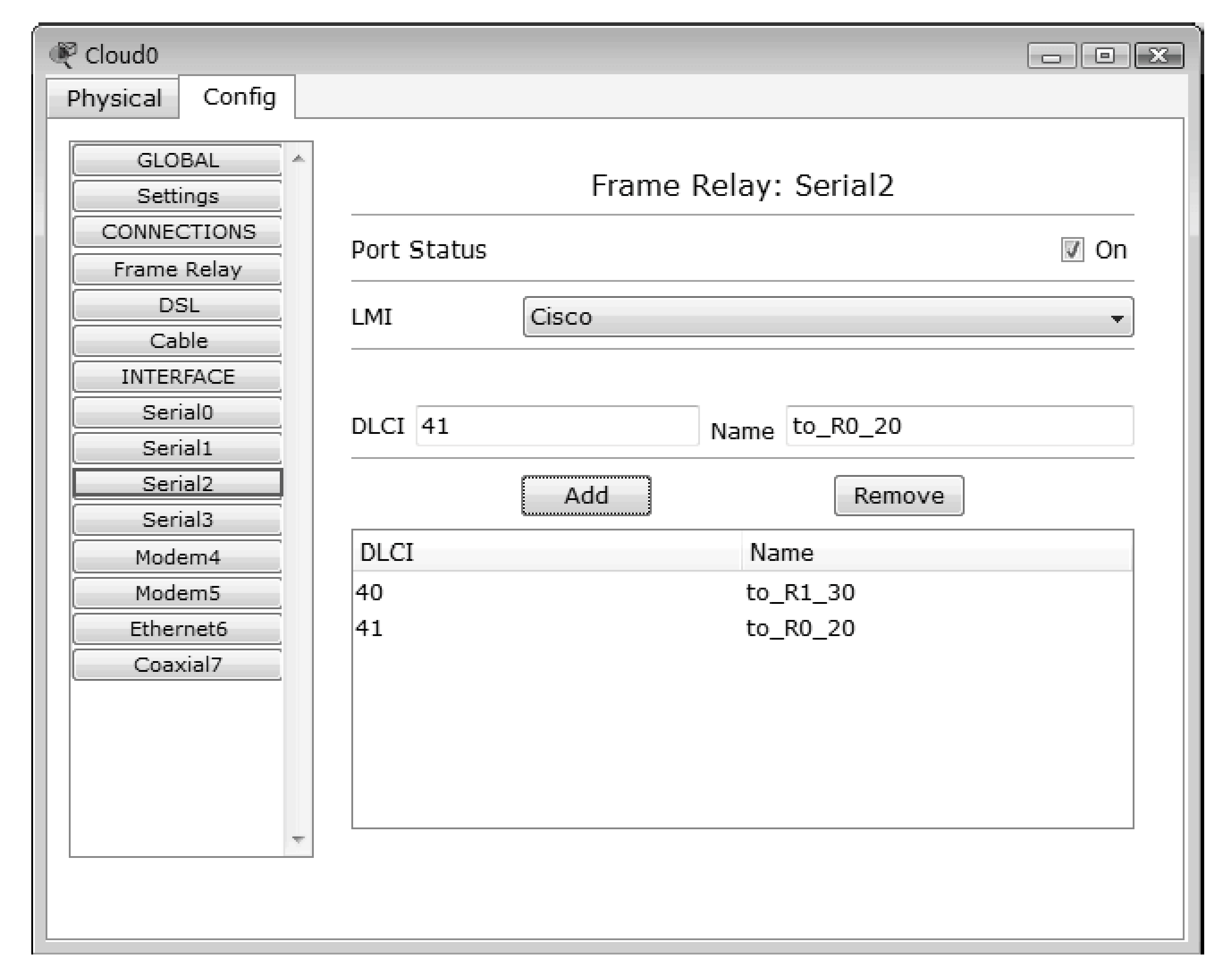
▲图 11-12　配置帧中继接口 Serial0 的 DLCI

（5）如图 11-13 所示，配置帧中继接口的 DLCI，选中 Serial1。DLCI 输入 30，Name 输入 to_R2_40，单击 Add 按钮，DLCI 输入 31，Name 输入 to_R0_21，单击 Add 按钮。



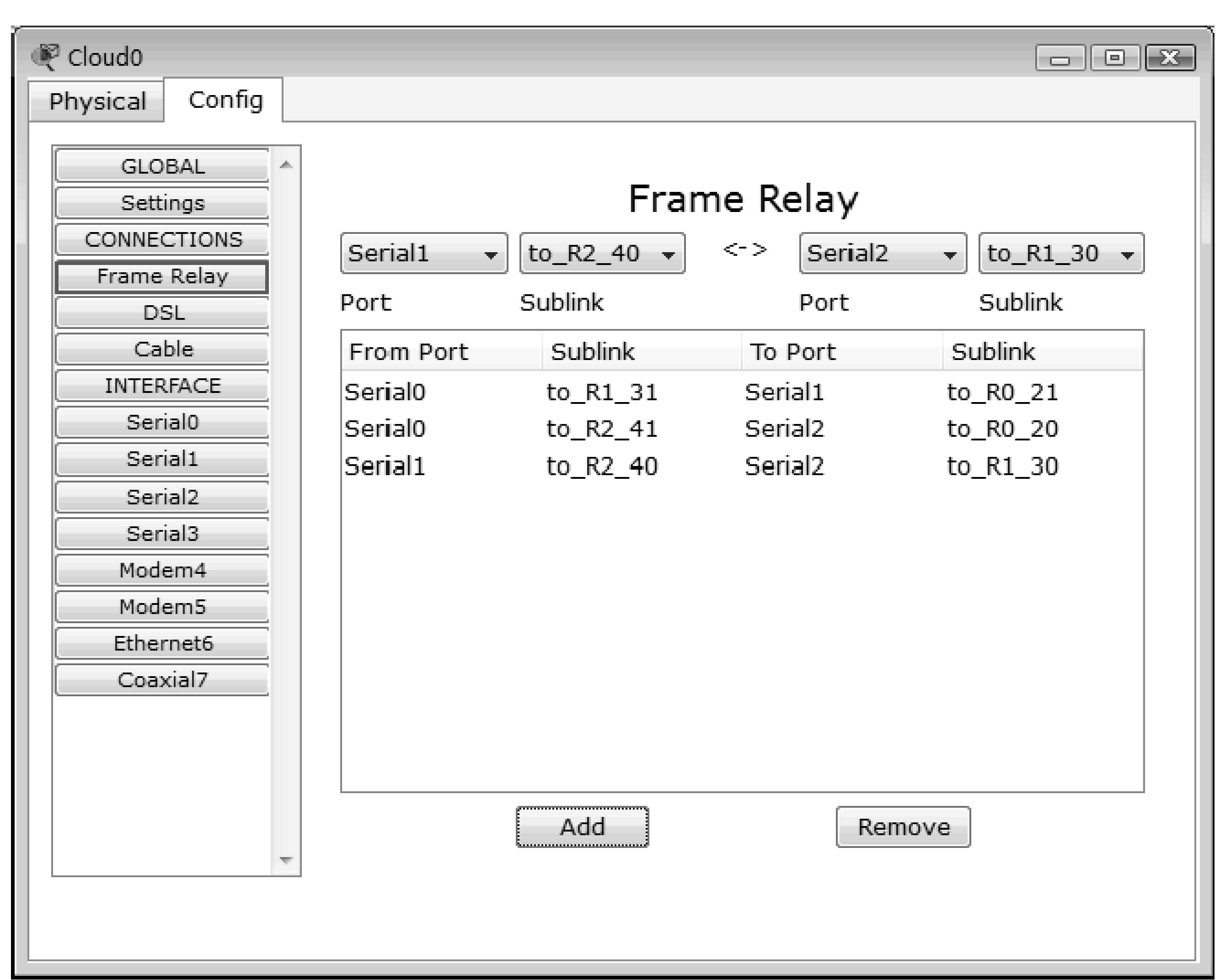
▲图 11-13　配置帧中继接口 Serial1 的 DLCI

（6）如图 11-14 所示，配置帧中继接口的 DLCI，选中 Serial2。DLCI 输入 40，Name 输入 to_R1_30，单击 Add 按钮；DLCI 输入 41，Name 输入 to_R0_20，单击 Add 按钮。



▲图 11-14 配置帧中继接口 Serial2 的 DLCI

（7）如图 11-15 所示，配置帧中继永久虚电路。选中 Serial0 接口的 to_R1_31 和 Serial1 接口的 to_R0_21，单击 Add 按钮，这就意味着从这两个接口建立了一条永久虚电路；选中 Serial0 接口的 to_R2_41 和 Serial2 接口的 to_R0_20，单击 Add 按钮，选中 Serial1 接口的 to_R2_40 和 Serial2 接口的 to_R1_30，单击 Add 按钮。



▲图 11-15 配置帧中继电路交换

（8）在 Router0 上验证帧中继配置。

```
Router0#show ip route
Codes: C - connected,S - static,I - IGRP,R - RIP,M - mobile,B - BGP
     D - EIGRP, EX - EIGRP external,O - OSPF,IA - OSPF inter area
     N1 - OSPF NSSA external type 1,N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1,E2 - OSPF external type 2,E - EGP
```

```
       i - IS-IS,L1 - IS-IS level-1,L2 - IS-IS level-2,ia - IS-IS inter area
       * - candidate default,U - per-user static route,o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    172.16.0.0/16 is directly connected, fastEthernet0/0
D    172.17.0.0/16 [90/2172416] via 192.168.2.1, 00:00:03, Serial0/1/0.2
D    172.18.0.0/16 [90/2172416] via 192.168.3.1, 00:05:13, Serial0/1/0.1
D    192.168.1.0/24 [90/2681856] via 192.168.2.1, 00:13:02, Serial0/1/0.2
                    [90/2681856] via 192.168.3.1, 00:07:30, Serial0/1/0.1
C    192.168.2.0/24 is directly connected, Serial0/1/0.2
C    192.168.3.0/24 is directly connected, Serial0/1/0.1
```

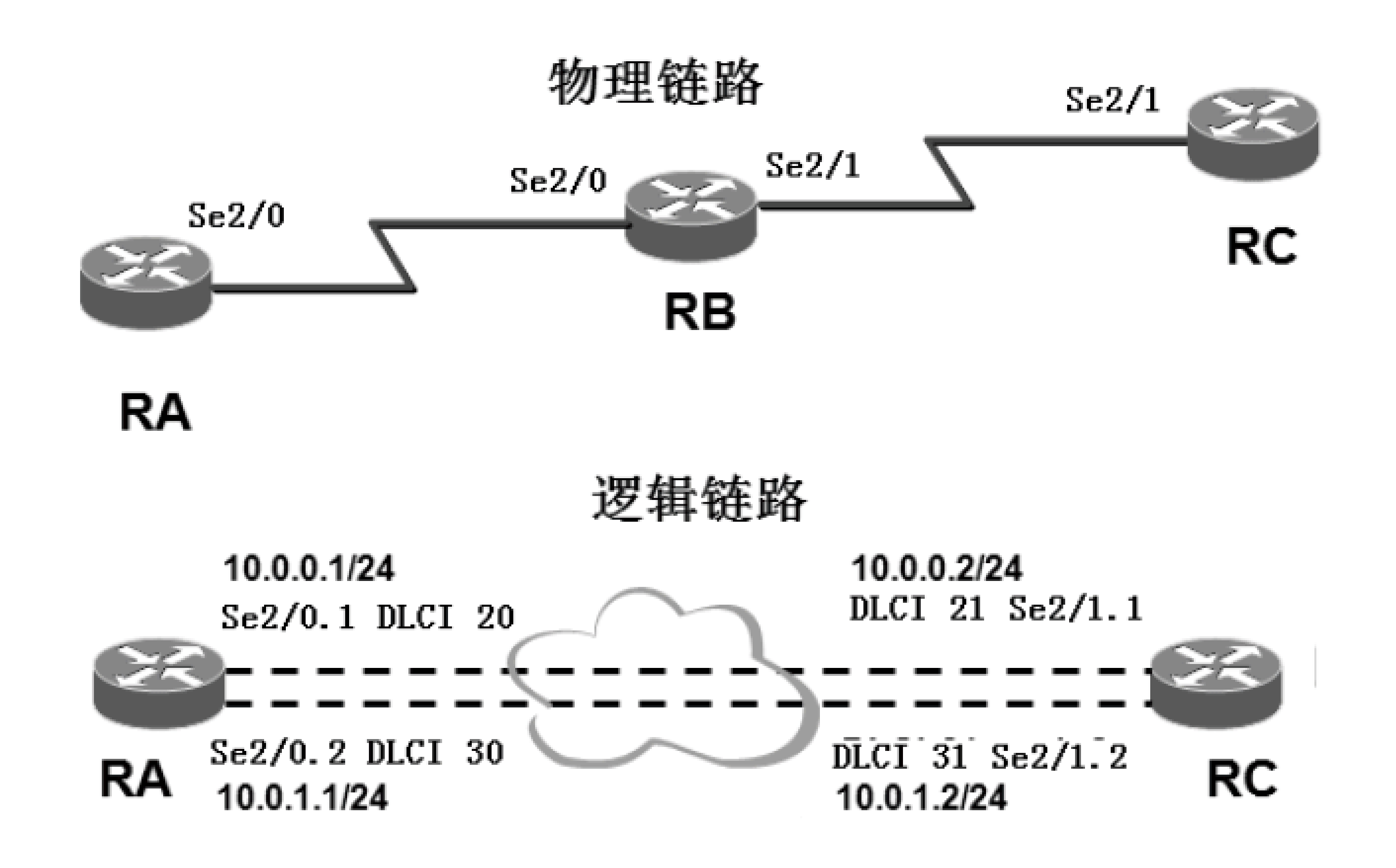
可以看到 Router0 已经学到了到达北京和天津网络的路由，说明帧中继配置成功。

说句实话，一般企业的网络管理员很少有机会配置帧中继网络，而更多的是配置路由器的广域网接口使用帧中继封装，然后配置子接口以及所对应帧中继的 DLCI。

3．将路由器配置为帧中继交换机

本实验会将路由器降级成为帧中继交换机，在帧中继交换机上配置两条永久虚电路，能够使得路由器 RA 和路由器 RB 相当于点到点的两个逻辑链路连接。各个子接口的 IP 地址和 DLCI 如图 11-16 所示，你需要配置路由器 RB 实现两个逻辑链路数据帧的转发。

通过本实验你将很好地理解在帧中继中配置永久虚电路的过程。



▲图 11-16　帧中继实验环境

操作步骤如下。

（1）在路由器 RA 上，配置广域网接口使用帧中继封装，配置子接口的 IP 地址以及对应的 DLCI。配置过程如图 11-17 所示。

```
Router>
Router>en
Router#config t
Router(config)#hostname RA
RA(config)#interface serial 2/0
RA(config-if)#no sh                                       物理端口配置帧中继封装
RA(config-if)#encapsulation frame-relay  ——  物理接口不要配置IP地址
RA(config-if)#exi
RA(config)#interface serial 2/0.1 point-to-point——进入子接口
RA(config-subif)#ip address 10.0.0.1 255.255.255.0
RA(config-subif)#frame-relay interface-dlci 20 ——指定DLCI编号
RA(config-fr-dlci)#ex
RA(config-subif)#exi
RA(config)#interface serial 2/0.2 point-to-point ——进入子接口
RA(config-subif)#ip address 10.0.1.1 255.255.255.0
RA(config-subif)#frame-relay interface-dlci 30 ——指定DLCI编号
RA(config-fr-dlci)#ex
```

▲图 11-17　在路由器 RA 上配置帧中继子接口

（2）在路由器 RB 上，将其配置为帧中继交换机，并在接口上配置帧中继封装以及永久虚电路，如图 11-18 所示。

```
Router>en
Router#config t
Router(config)#hostname RB
RB(config)#frame-relay switching ——将路由器降级为帧中继交换机
RB(config)#interface serial 2/0
RB(config-if)#encapsulation frame-relay        配置帧中继封装且为DCE
RB(config-if)#frame-relay intf-type dce        配置时钟频率
RB(config-if)#clock rate 64000
RB(config-if)#frame-relay route 20 interface serial 2/1 21   配置帧中继映射
RB(config-if)#frame-relay route 30 interface serial 2/1 31   即配置永久虚电路
RB(config-if)#ex
RB(config)#interface serial 2/1                 配置帧中继封装且为DCE
RB(config-if)#encapsulation frame-relay         配置时钟频率
RB(config-if)#frame-relay intf-type dce
RB(config-if)#clock rate 64000
RB(config-if)#frame-relay route 31 interface serial 2/0 30   配置帧中继映射
RB(config-if)#frame-relay route 21 interface serial 2/0 20   即配置永久虚电路
```

▲图 11-18　配置帧中继交换机

路由器 RB 原本是三层设备，现在将其作为帧中继交换机，成为了二层设备，因此是降级使用。在接口上配置帧中继映射的过程就是在帧中继交换机上创建永久虚电路的过程。

（3）在路由器 RC 上，配置广域网接口使用帧中继封装，配置子接口的 IP 地址以及对应的 DLCI，如图 11-19 所示。

```
RC(config)#interfac serial 2/1
RC(config-if)#encapsulation frame-relay ——配置物理接口
                                          帧中继封装
RC(config-if)#no sh
RC(config-if)#exi
RC(config)#interface serial 2/1.1 point-to-point
RC(config-subif)#ip address 10.0.0.2 255.255.255.0   配置子接口IP
RC(config-subif)#frame-relay interface-dlci 21       和DLCI
RC(config-fr-dlci)#ex
RC(config-subif)#no sh
RC(config)#interface serial 2/1.2 point-to-point     配置子接口IP
RC(config-subif)#ip address 10.0.1.2 255.255.255.0   和DLCI
RC(config-subif)#frame-relay interface-dlci 31
RC(config-fr-dlci)#^Z
```

▲图 11-19　在路由器 RC 上配置帧中继子接口

（4）在路由器 RA 上查看子接口状态。可以看到物理层和数据链路层都是 up 状态，帧中继封装，如图 11-20 所示。

```
RA#show interfaces serial 2/0.1
Serial1/0.1 is up, line protocol is up
  Hardware is M4T
  Internet address is 10.0.0.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never
RA#show interfaces serial 2/0.2
Serial1/0.2 is up, line protocol is up
  Hardware is M4T
  Internet address is 10.0.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never
```

▲图 11-20　查看帧中继子接口

（5）在路由器 RA 上测试到 RC 的两个逻辑接口是否通，如果通，说明帧中继的两个永久虚电路配置成功，如图 11-21 所示。

```
RA#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 216/395/504 ms

RA#ping 10.0.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 216/342/564 ms
```

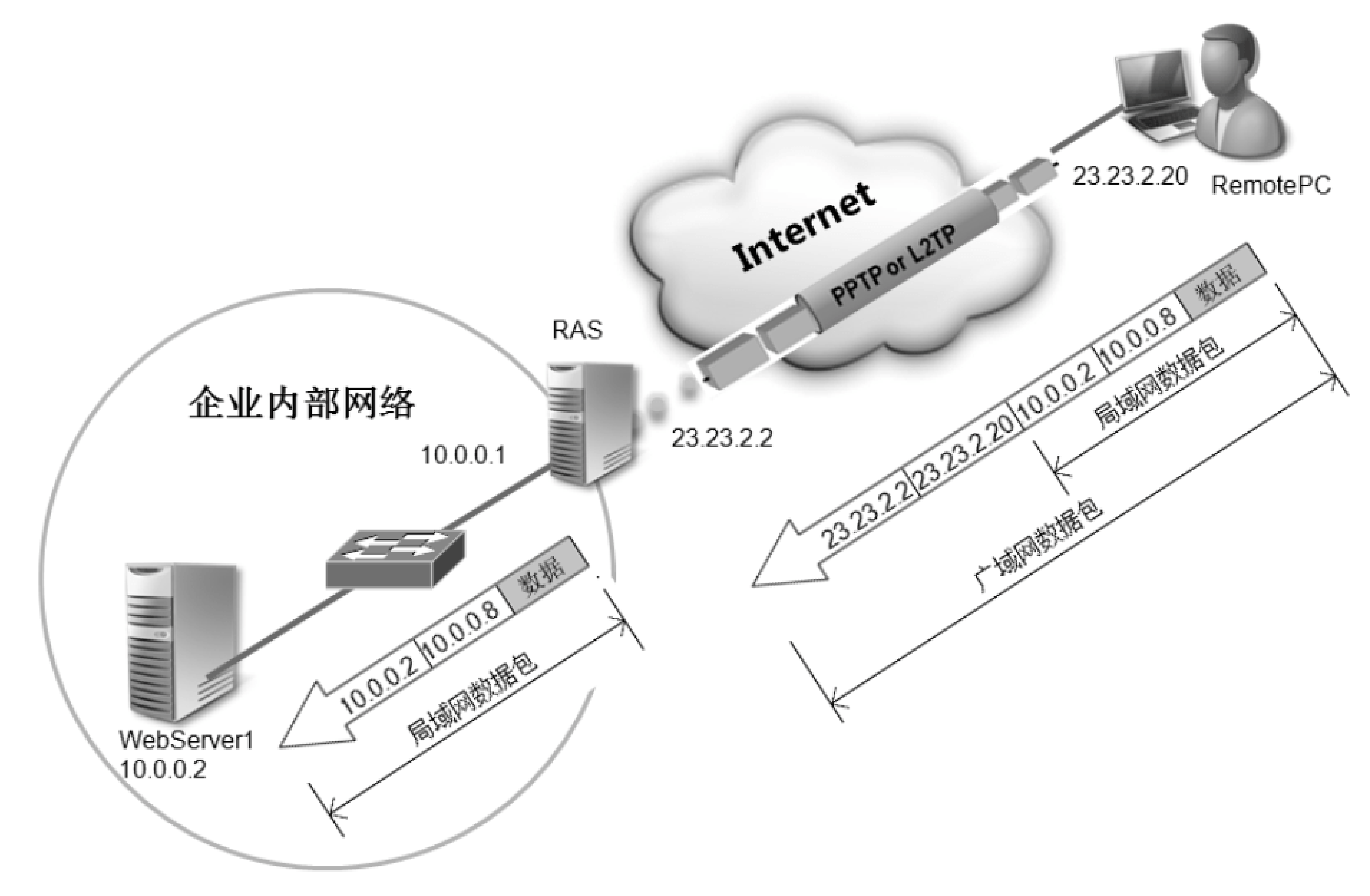
▲图 11-21　测试网络连通性

11.3 虚拟专用网

虚拟专用网络（VPN，Y）我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊加密的通信协议连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专用的通信线路，如同架设了一条专线，但是它并不需要真正地去铺设光缆之类的物理线路。这好比去电信局申请专线，但是不用付铺设线路的费用，也不用购买路由器等硬件设备。VPN 技术原是路由器具有的重要技术之一，目前交换机、防火墙设备以及 Windows 2003 和 Windows Server 2003 等软件中也都支持 VPN。总之，VPN 的核心就是利用公共网络建立虚拟私有网。

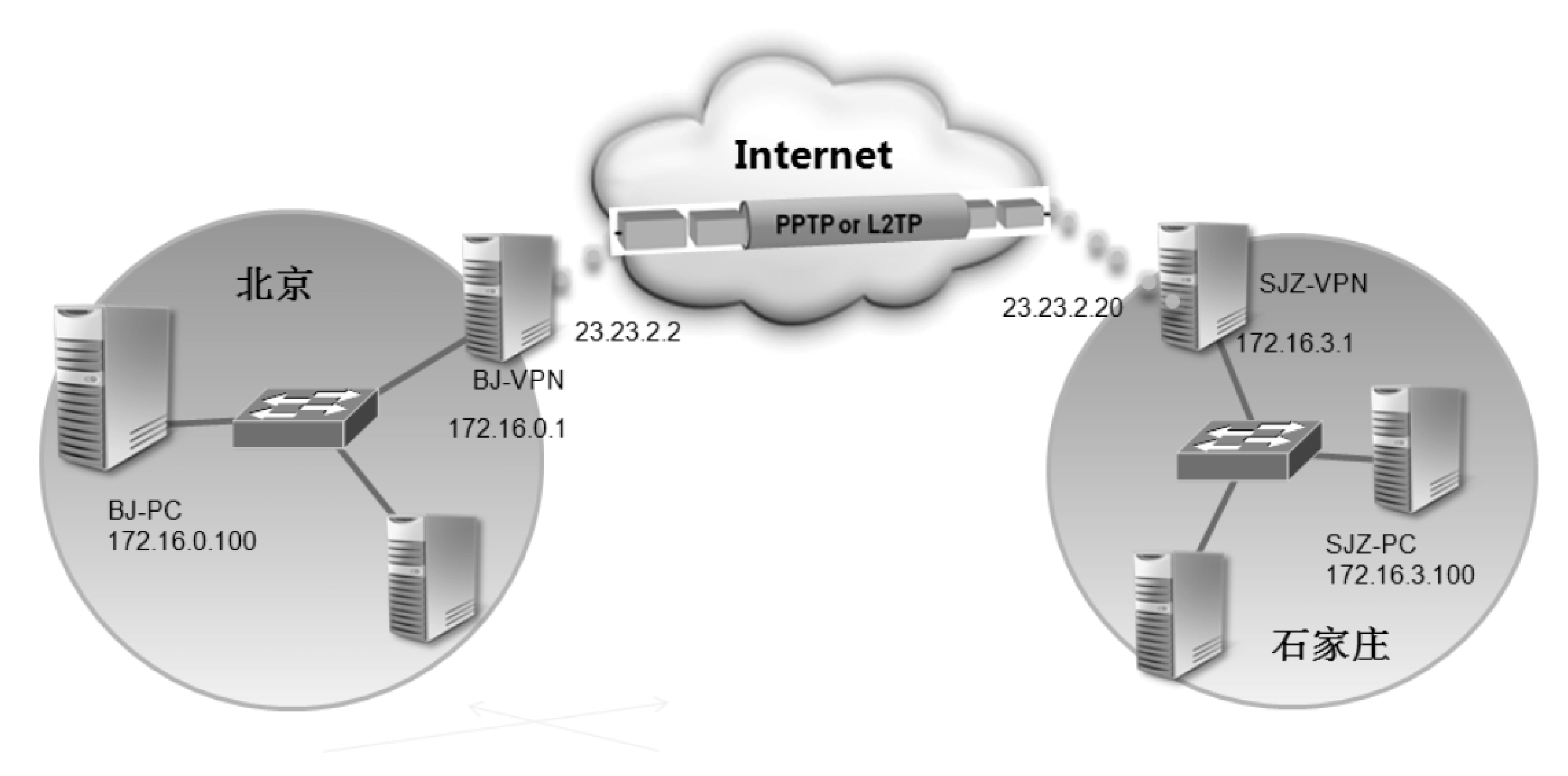
如图 11-22 所示的远程用户可以通过 Internet 建立到企业内部网络的 VPN 连接，这样该用户就可以像是在内网中一样访问企业内部网络的任意计算机。远程用户建立到 RAS（Remote Access Server）服务器的 VPN 拨号连接后，会得到一个内网的 IP 地址 10.0.0.8。当它访问内网的 WebServer1 时，数据包的封装如图 11-21 所示，将会把局域网的数据包当做数据，使用 RAS 的公网地址和自己的公网地址再次封装为广域网数据包，这样数据包就能通过 Internet 到达 RAS 的公网地址 23.23.2.2。RAS 再将广域网封装的部分去掉，使局域

网数据包在企业内部网络传输。这里省去了广域网封装过程中数据包加密和完整性的封装介绍。



▲图 11-22　远程访问 VPN 示意图

还有一种 VPN 是站点间 VPN，如图 11-23 所示。站点间 VPN 可以通过 Internet 将两个局域网连接起来，你只需配置北京和石家庄两个局域网的 VPN 服务器即可，对于北京和石家庄内网的计算机相互访问 Internet 则是透明的。



▲图 11-23　站点间 VPN 示意图

通过以上介绍可以看出，VPN 技术是利用 Internet 扩展私有网络的一项非常有用的技术，它不需要额外的开销，利用现有的 Internet 接入，只需稍加配置就能实现远程用户对内网的访问以及两个私有网络的相互访问。

下面将会介绍 VPN 使用的广域网协议以及如何在路由器和 Windows Server 2003 上实现远程访问 VPN。

11.3.1 VPN 使用的广域网协议

VPN 中的隧道是由隧道协议形成的。VPN 使用的隧道协议主要有两种：点到点隧道协议（PPTP）和第二层隧道协议（L2TP over IPSec）。

PPTP 封装了 PPP 数据包中包含的用户信息，支持隧道交换。隧道交换可以根据用户权限，开启并分配新的隧道，将 PPP 数据包在网络中传输。另外，隧道交换还可以将用户导向指定的企业内部服务器。PPTP 便于企业在防火墙和内部服务器上实施访问控制。位于企业防火墙的隧道终端器接收包含用户信息的 PPP 数据包，然后对不同来源的数据包实施访问控制。

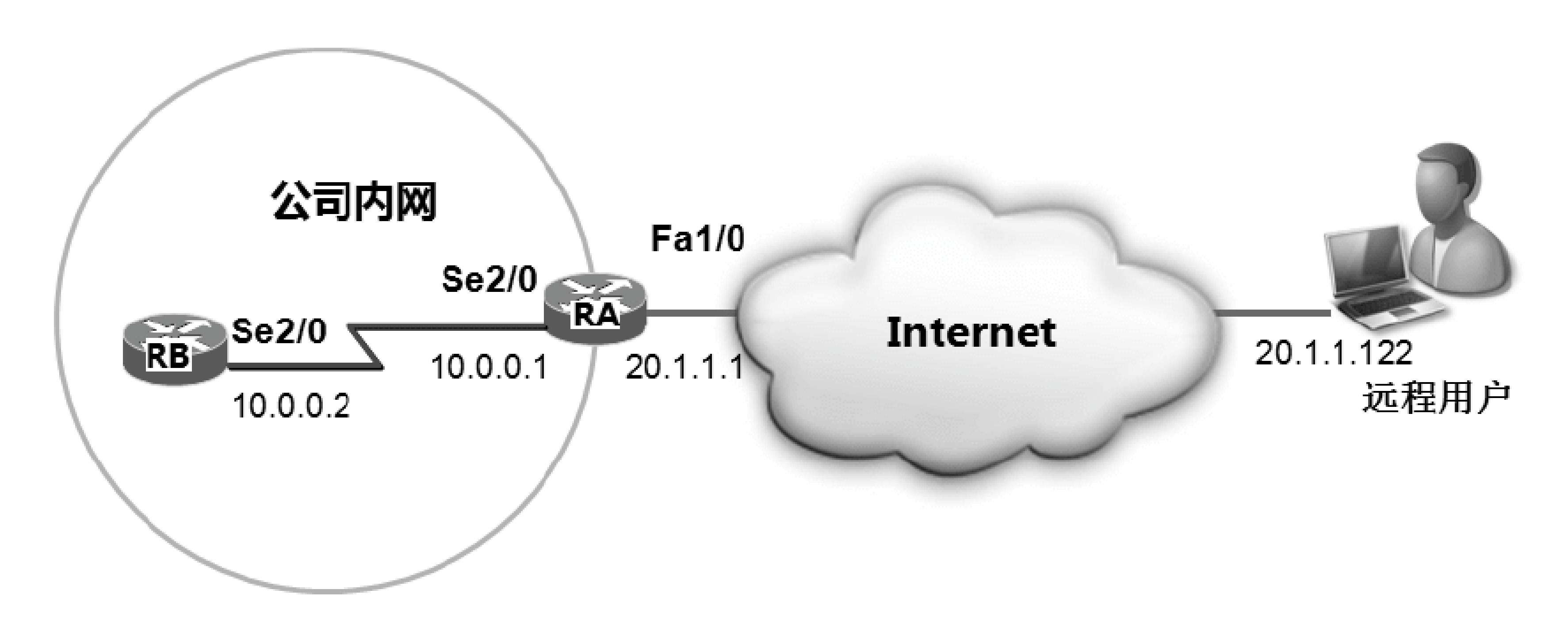
L2TP 协议综合了 PPTP 协议和 L2F（Layer 2 Forwarding）协议的优点，并且支持多路隧道，这样可以使用户同时访问 Internet 和企业网，但需要结合 IPSec 实现其安全性。

PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加附加报头用于数据在互联网络上的传输。尽管两个协议非常相似，但仍存在以下几方面的不同。

- PPTP 要求互联网络为 IP 网络；L2TP 只要求隧道媒介提供面向数据包的点对点连接。L2TP 可以在 IP（使用 UDP）、帧中继永久虚拟电路（PVCs）、X.25 虚拟电路（VCs）或 ATM VCs 网络上使用。
- PPTP 只能在两端点间建立单一隧道；L2TP 支持在两端点间使用多隧道，使用 L2TP，用户可以针对不同的服务质量创建不同的隧道。
- L2TP 可以提供包头压缩，当压缩包头时，系统开销（overhead）占用 4 个字节；而 PPTP 协议下要占用 6 个字节。
- L2TP 可以提供隧道验证；而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，不需要在第 2 层协议上验证隧道。
- PPTP 使用 TCP 的 1723 端口；L2TP 使用 UDP 的 1701 端口。

11.3.2 配置路由器为 VPN 服务器

下面用 Cisco 3660 系列路由器配置为远程访问服务器，允许 Internet 用户通过 L2TP 协议拨入到企业内网。本实验需要 Dynamips 软件搭建的网络环境，网络拓扑如图 11-24 所示，路由器 RB 模拟企业内网的一个计算机，在路由器 RA 上配置远程访问服务器，远程用户使用虚拟机来模拟。



▲图 11-24　远程访问 VPN 实验环境

按照图 11-23 所示配置路由器 RA 和路由器 RB 的 IP 地址，以及远程计算机的 IP 地址。在路由器 RB 上添加默认路由。

```
RB（cofnig）#ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

1. 在 RA 上配置 L2TP VPN

（1）如图 11-25 所示，在 LNS 上配置远程用户拨入的用户名和对应的密码。

```
RA(config)#username han password p@ssw0rd
```

▲图 11-25　配置远程拨入用户

（2）如图 11-26 所示，启用 VPDN 功能（VPDN 默认是关闭的）。

```
RA(config)#vpdn enable
```

▲图 11-26　启用 VPDN 功能

（3）vpdn-group onest-l2tp：建立一个虚拟拨号组，并命名为 onest-l2tp。

accept-dialin：设置允许客户端拨入。

protocol l2tp：启用 l2TP 隧道协议。

virtual-template 1：建立一个虚拟接口 1（一个虚拟拨号组中最多可以建立 25 个虚拟接口）。

配置过程如图 11-27 所示。

```
RA(config)#vpdn-group onest-l2tp
RA(config-vpdn)#accept-dialin
RA(config-vpdn-acc-in)#protocol l2tp
RA(config-vpdn-acc-in)#virtual-template 1
RA(config-vpdn-acc-in)#exi
```

▲图 11-27　建立和配置虚拟拨号组

（4）关闭 l2TP 隧道的认证功能（也可以开启认证功能，这时候，需要搭建一台 CA，然后申请证书，并且客户端也需要申请证书才能连上 RA，这样会更安全）。配置过程如图 11-28 所示。

```
RA(config-vpdn)#no l2tp tunnel authentication
RA(config-vpdn)#exi
```

▲图 11-28　关闭 L2TP 隧道认证功能

（5）建立 VPN 客户端拨入分配的 IP 地址的地址池，并命名为 onest-l2tp-user。也可以通过企业内部 DHCP 服务器申请，如图 11-29 所示。

```
RA(config)#ip local pool onest-l2tp-user 172.16.0.1 172.16.0.100
```

▲图 11-29　指定分配各远程计算机的地址池

（6）interface virtual-Template 1：进入虚拟拨号组 onest-myl2tp 的虚拟接口 1。

（7）ip unnumbered fastEthernet 1/0：借用出口端口 fastEthernet 1/0 的接口来转发 l2TP 隧道协议传输的流量。

（8）peer default ip address pool onest-l2tp-user：设置 VPN Client 拨号动态获得 IP 地址对应的地址池。

（9）设置客户端拨入 LNS 服务器需要的认证方式为 chap ms-chap。配置过程如图 11-30 所示。

```
RA(config)#interface virtual-Template 1
RA(config-if)#ip unnumbered fastEthernet 1/0
RA(config-if)#peer default ip address pool onest-l2tp-user

RA(config-if)#ppp authentication ?
  chap        Challenge Handshake Authentication Protocol (CHAP)
  eap         Extensible Authentication Protocol (EAP)
  ms-chap     Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
  ms-chap-v2  Microsoft CHAP Version 2 (MS-CHAP-V2)
  pap         Password Authentication Protocol (PAP)

RA(config-if)#ppp authentication chap ms-chap
```

▲图 11-30　配置虚拟拨号组 1

（10）如图 11-31 所示，配置完成之后，在 LNS 上通过 show ip interface brief 查看虚拟拨号接口 Virtual-Template1 的 IP 地址，可以看出是借用了 FastEthernet1/0 的 IP 地址。

```
RA(config-if)#^Z
RA#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES unset  administratively down down

FastEthernet0/1            unassigned      YES unset  administratively down down

FastEthernet1/0            20.1.1.1        YES manual up                    up

Serial2/0                  10.0.0.1        YES manual up                    up

Serial2/1                  unassigned      YES unset  administratively down down

Serial2/2                  unassigned      YES unset  administratively down down

Serial2/3                  unassigned      YES unset  administratively down down

Virtual-Access1            unassigned      YES unset  down                  down

Virtual-Template1          20.1.1.1        YES TFTP   down                  down
```

▲图 11-31　查看配置的 Virtual-Template 接口

2. 配置 VPN 客户端

（1）如图 11-32 所示，确保 Internet 上的计算机能够 ping 通 RA 路由器的 Fa1/0 接口。

```
C:\Documents and Settings\han>ping 20.1.1.1

Pinging 20.1.1.1 with 32 bytes of data:

Reply from 20.1.1.1: bytes=32 time=198ms TTL=255
Reply from 20.1.1.1: bytes=32 time=157ms TTL=255
Reply from 20.1.1.1: bytes=32 time=23ms TTL=255
Reply from 20.1.1.1: bytes=32 time=94ms TTL=255

Ping statistics for 20.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 198ms, Average = 118ms
```

▲图 11-32　测试到远程访问服务器 RA 的连通性

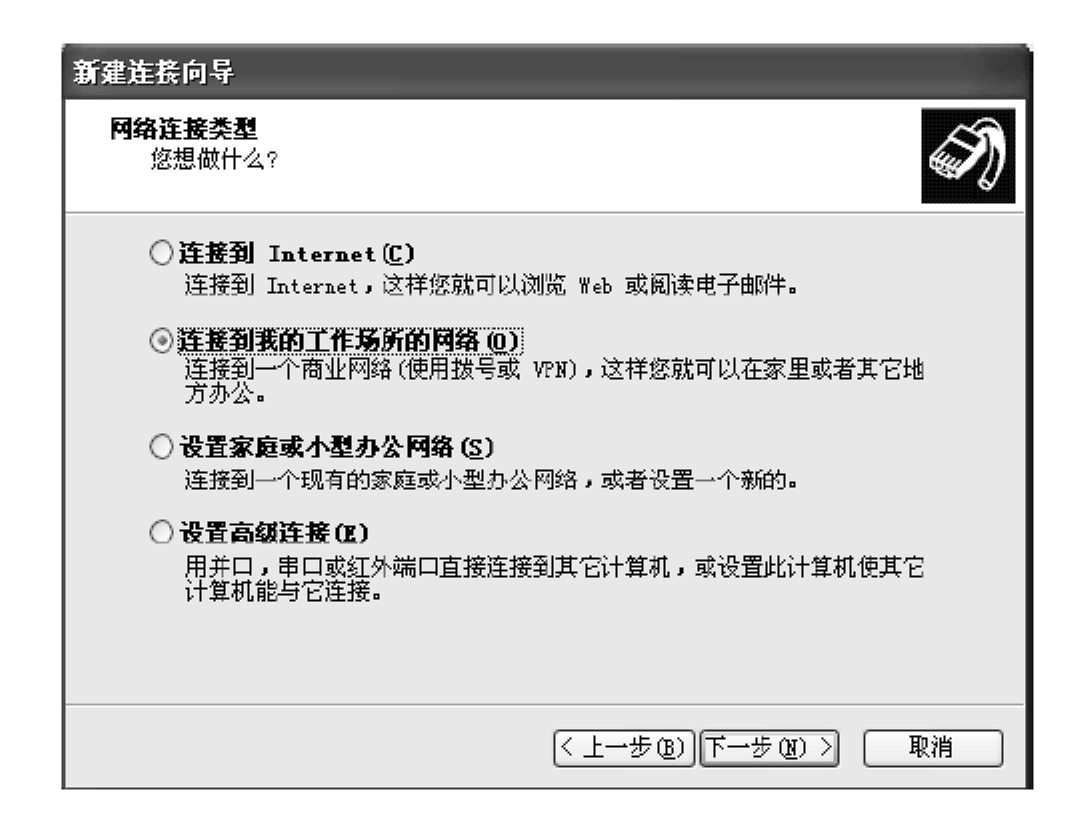
（2）如图 11-33 所示，在计算机中打开“网络连接”窗口，单击“创建一个新的连接”，建立 VPN 拨号连接。



▲图 11-33　创建 VPN 拨号连接

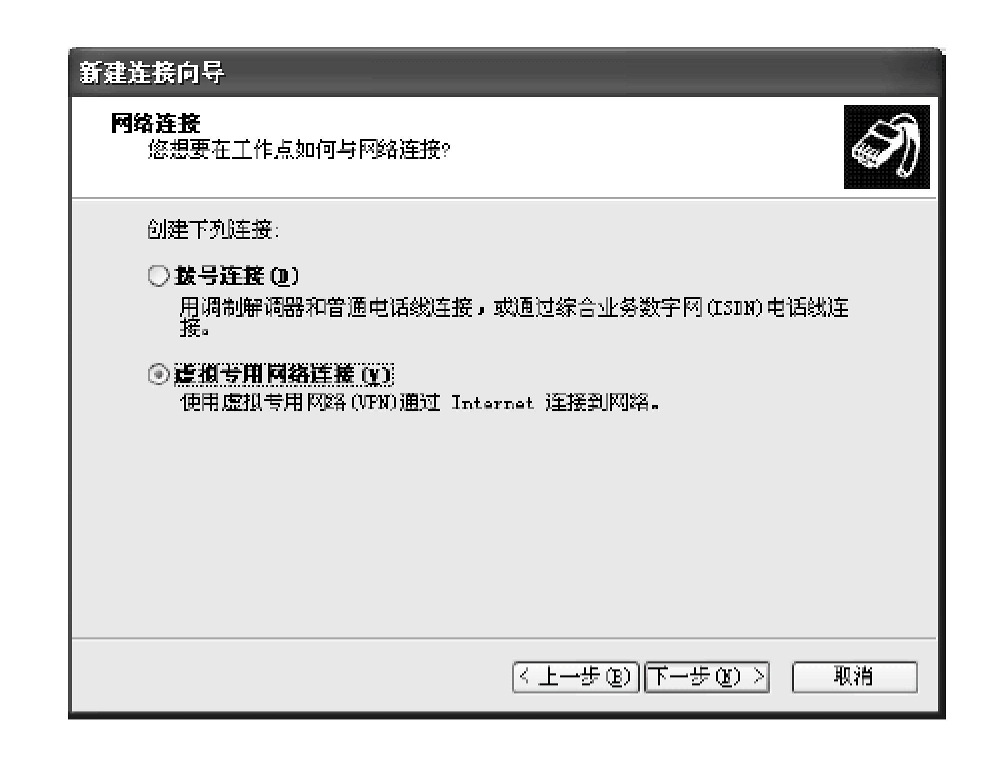
（3）在出现的“欢迎使用新建连接向导”对话框中，单击“下一步”按钮。

（4）如图 11-34 所示，在出现的“网络连接类型”设置界面中，选中“连接到我的工作场所的网路”单选按钮，单击“下一步”按钮。



▲图 11-34　选择网络连接类型

（5）如图 11-35 所示，在出现的“网络连接”设置界面中，选中“虚拟专用网络连接”单选按钮，单击“下一步”按钮。



▲图 11-35　选择网络连接

（6）如图 11-36 所示，在出现的“连接名”设置界面中，输入名称，单击“下一步”按钮。



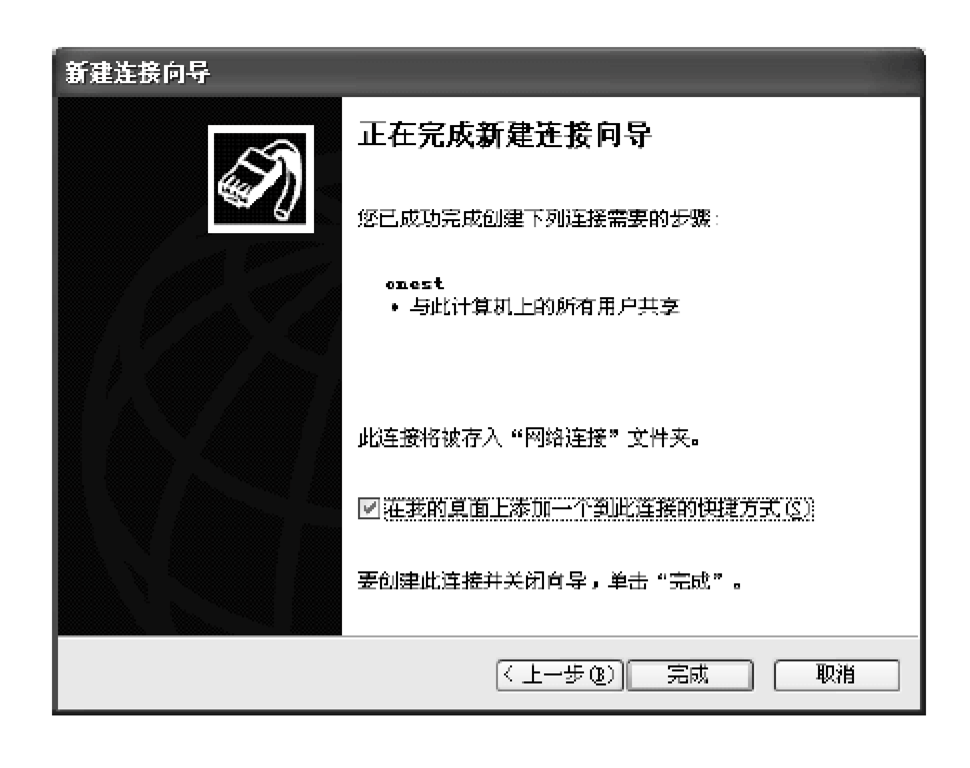
▲图 11-36　指定连接名称

（7）如图 11-37 所示，在出现的“VPN 服务器选择”设置界面中，输入远程访问服务器的地址。在这里就是路由器 RB 连接 Internet 的 IP 地址，单击“下一步”按钮。



▲图 11-37　输入远程访问服务器的 IP 地址

（8）如图 11-38 所示，在出现的“正在完成新建连接向导”设置界面中，选中“在我的桌面上添加一个到此连接的快捷方式”复选框，单击“完成”按钮。



▲图 11-38　完成 VPN 拨号创建

（9）如图 11-39 所示，右击刚才创建的 VPN 拨号连接，在弹出的快捷菜单中选择“属性”命令。

（10）如图 11-40 所示，在出现的属性对话框的“安全”选项卡中，选中“高级”单选按钮。单击“设置”按钮。




▲图 11-39　更改拨号连接的属性



▲图 11-40　更改安全设置

（11）如图 11-41 所示，在出现的“高级安全设置”对话框中，选中“允许这些协议”单选按钮，并选中“质询握手身份验证协议”复选框和 Microsoft CHAP 复选框，取消选中“Microsoft CHAP 版本 2”复选框，单击“确定”按钮。



▲图 11-41　更改高级安全设置

（12）如图 11-42 所示，在“网络”选项卡中的“VPN 类型”下拉列表框中选择 L2TP IPSec VPN 选项，单击“确定”按钮。完成配置。



▲图 11-42　更改 VPN 类型

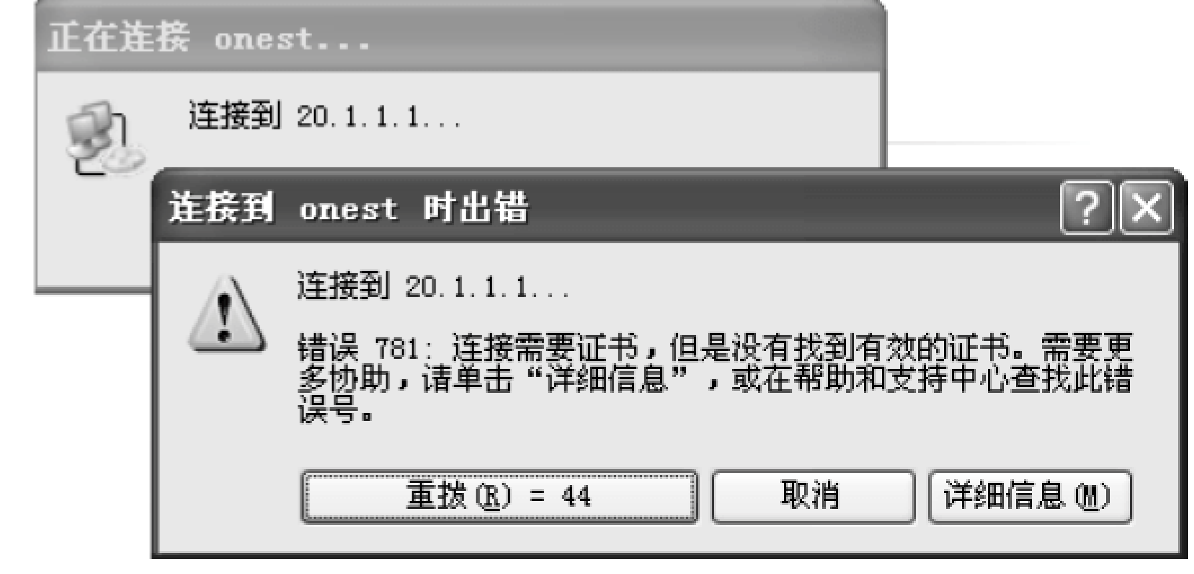
（13）如图 11-43 所示，设置完成之后，输入用户名和密码（在 RA 服务器上设置的用户名和密码）连接 RA 服务器。

（14）如图 11-44 所示，连接过程中会出现需要证书的错误，这是因为 Windows 2000/XP/2003 的 L2TP 默认启动证书方式的 IPSec，所以必须向 Windows 添加 ProbibitIpSec 注册表值，以防止创建用于 L2TP/IPSec 通信的自动筛选器。

ProbibitIpSec 注册表值设置为 1 时，基于 Windows 2000 的计算机不会创建使用 CA 身份验证的自动筛选器，而是检查本地 IPSec 策略或 Active Directory IPSec 策略。



▲图 11-43　输入用户名和密码



▲图 11-44　需要证书

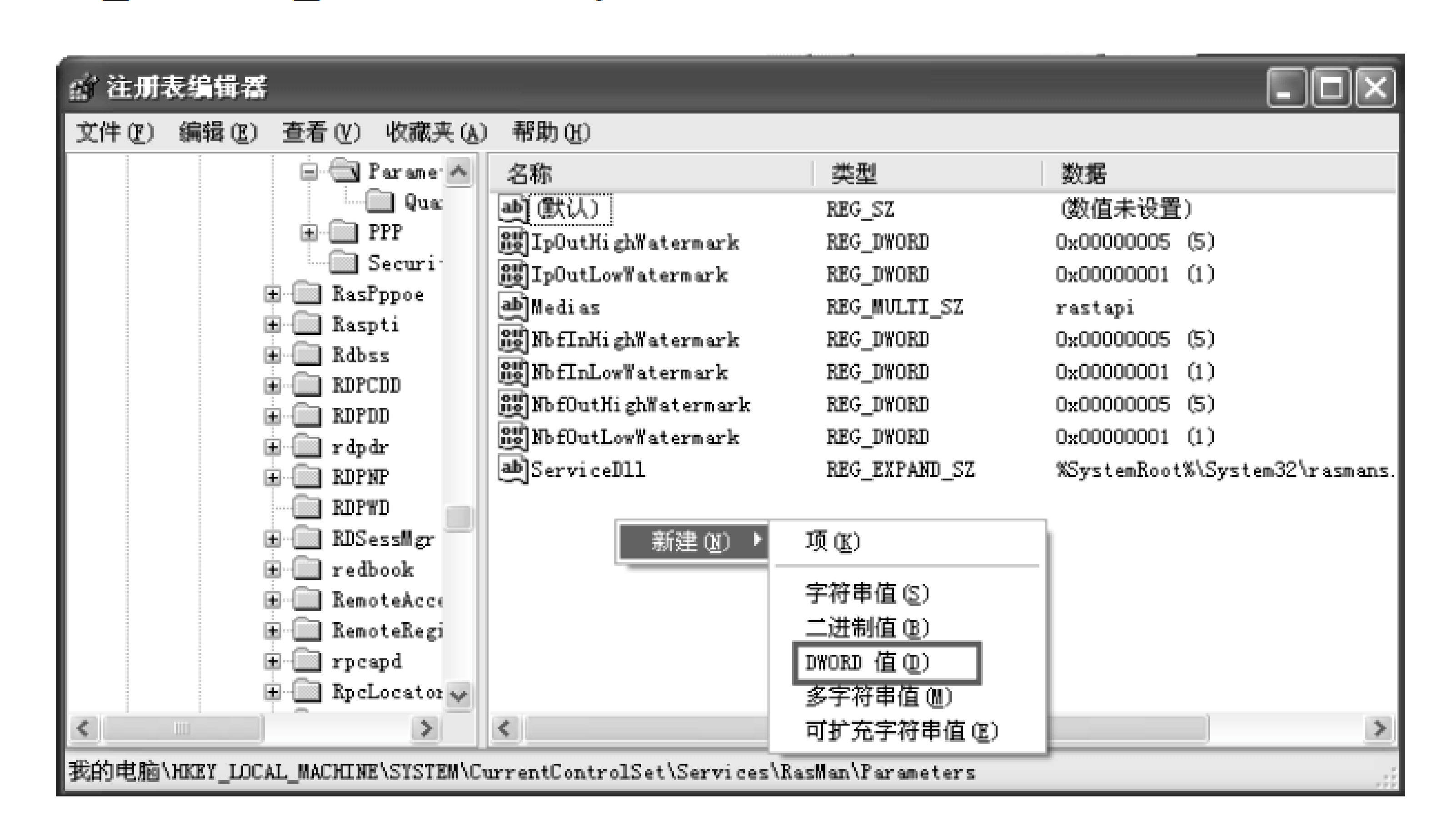
3. 修改 VPN 客户端的注册表

要向 Windows 添加 ProbibitIpSec 注册表值，请按照下列步骤操作。

（1）选择“开始”→“运行”命令，在弹出的“运行”对话框中输入 regedit，然后单击“确定”按钮。

（2）如图 11-45 所示，找到下面的注册表子项，然后单击它：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters



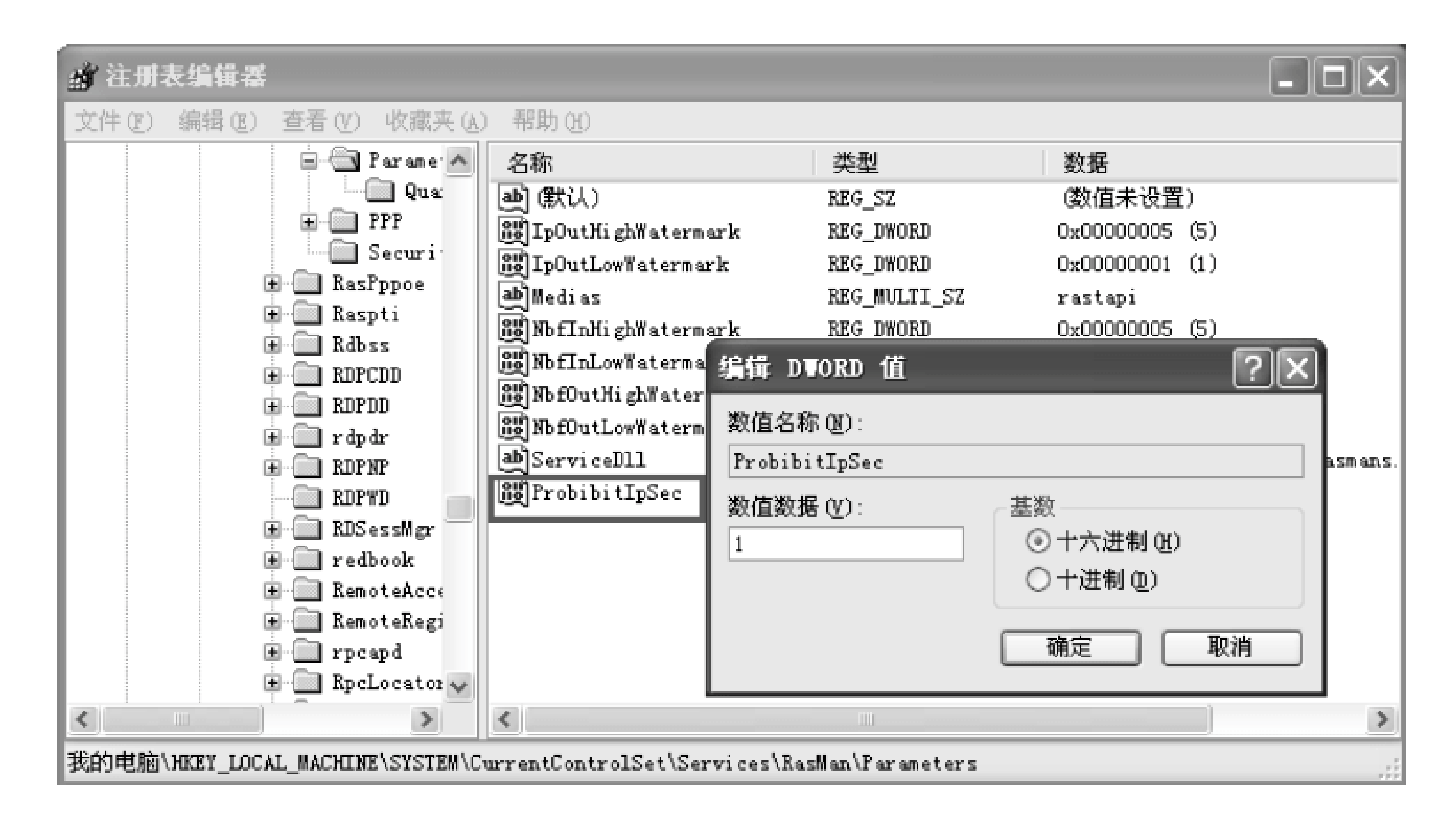
▲图 11-45　创建注册表项

（3）在该项中新建一个“DWORD 值”。

（4）将 DWORD 值重命名为 ProbibitTpSec。

（5）如图 11-46 所示，双击 ProbibitTpSec，将其值更改为 1。

（6）退出注册表编辑器，然后重新启动计算机。



▲图 11-46　更改键值

4. 拨号之后访问内网

（1）如图 11-47 所示，拨号之后查看 IP 配置，可以看到 VPN 拨号后远程访问服务器分配的内网地址 172.16.0.1。

```
C:\Documents and Settings\han>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 20.1.1.122
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

PPP adapter onest:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.0.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 172.16.0.1
```

▲图 11-47　查看拨号后建立的连接

（2）如图 11-48 所示，访问内网路由器 RB 的地址

```
C:\Documents and Settings\han>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=149ms TTL=254
Reply from 10.0.0.2: bytes=32 time=56ms TTL=254
Reply from 10.0.0.2: bytes=32 time=101ms TTL=254
Reply from 10.0.0.2: bytes=32 time=69ms TTL=254

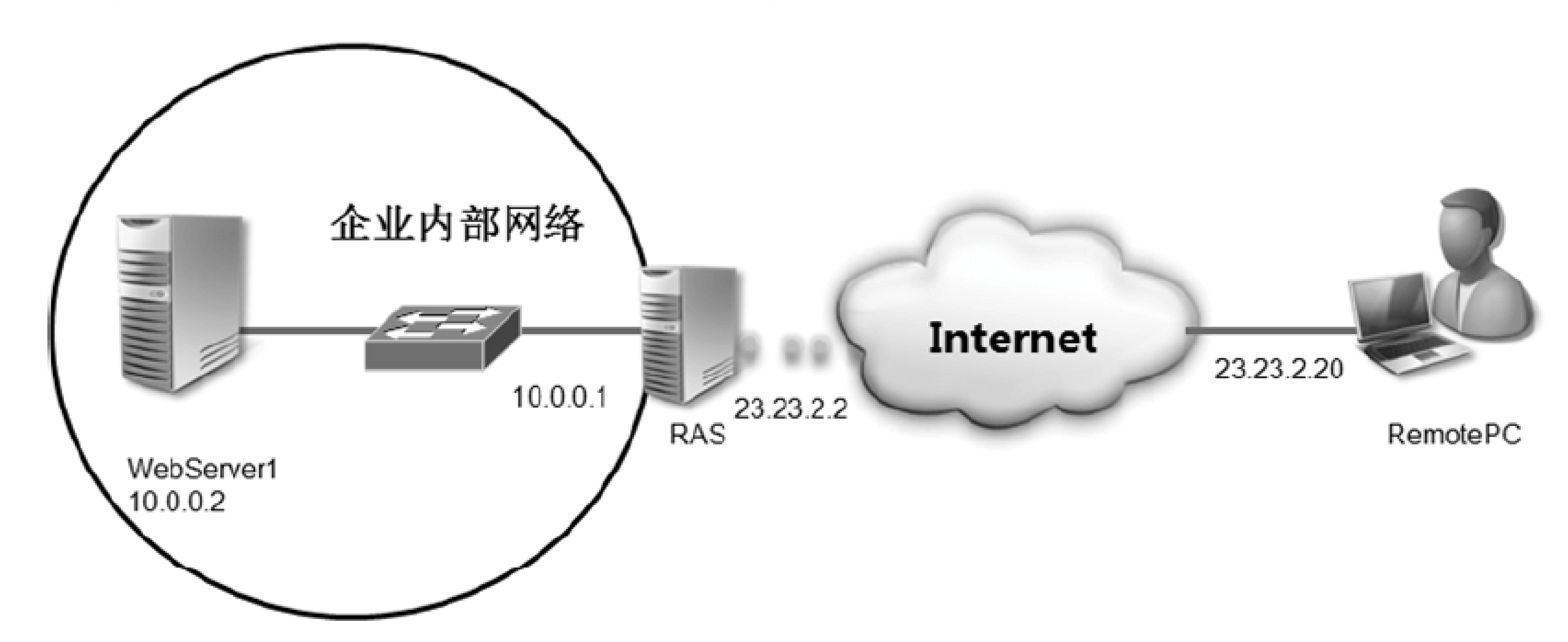
Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 56ms, Maximum = 149ms, Average = 93ms
```

▲图 11-48　测试到内网的访问

（3）断开 VPN 拨号，你将不能访问内网的计算机。

11.3.3　配置 Windows 服务器为 VPN 服务器

如图 11-49 所示，企业内网地址为 10.0.0.0/24，RAS 为 Windows Server 2003 服务器，连接内网和外网。现在需要配置 RAS 服务器为远程访问服务器，允许 Internet 用户能够拨入内网。



▲图 11-49　远程访问 VPN 示意图

在 Windows Server 2003 上配置远程访问服务器的步骤如下。

（1）启用路由和远程访问服务器。

（2）指定分配给远程计算机的 IP 地址。

（3）创建用户允许远程拨入。

1．配置远方访问服务器的

在 RAS 上，按照图 11-48 所示配置连接 Internet 和内网的 IP 地址。

（1）选择“开始”→“程序”→“管理工具”→“路由和远程访问”命令。

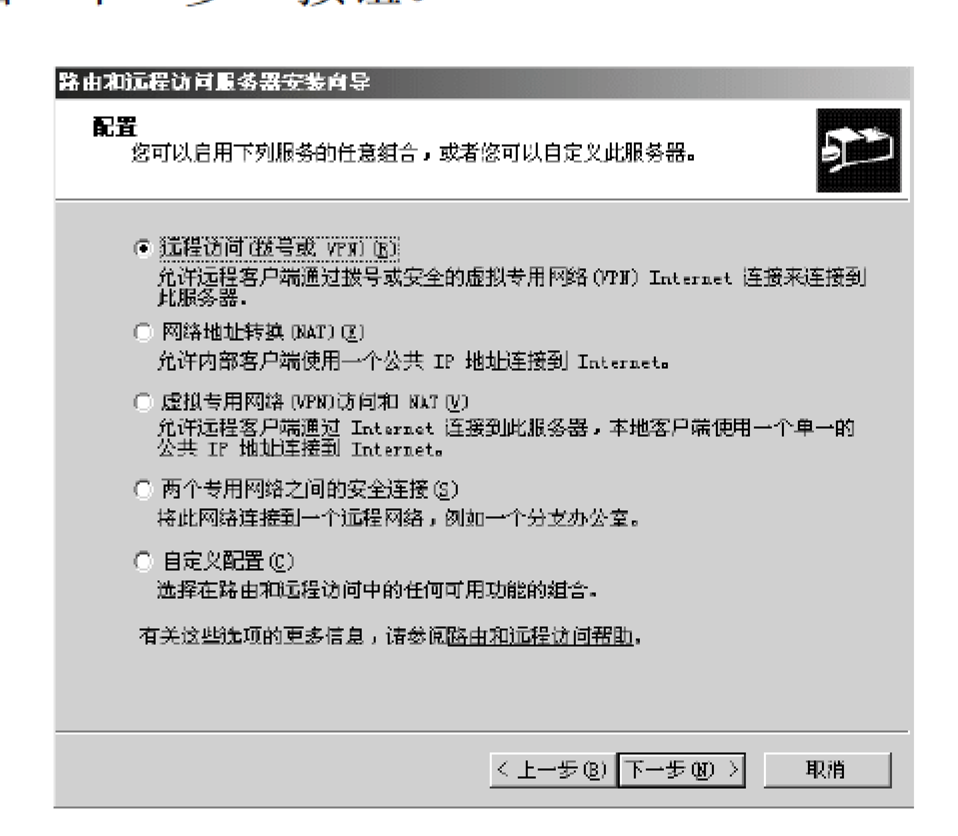
（2）如图 11-50 所示，右击服务器，在弹出的快捷菜单中选择“配置路由和远程访问”命令。



▲图 11-50　配置路由和远程访问

（3）在出现的“欢迎使用路由和远程访问服务器安装向导”对话框中，单击“下一步”按钮。

（4）如图 11-51 所示，在出现的“配置”设置界面中，选中“远程访问（拨号或 VPN）”单选按钮，单击“下一步”按钮。



▲图 11-51　选择远程访问

（5）如图 11-52 所示，在出现的“远程访问”设置界面中，选中 VPN 复选框，单击“下一步”按钮。



▲图 11-52　选择 VPN 连接

（6）如图 11-53 所示，在出现的“VPN 连接”设置界面中，选中连接 Internet 的网卡，单击“下一步”按钮。



▲图 11-53　选择连接 Internet 的网卡

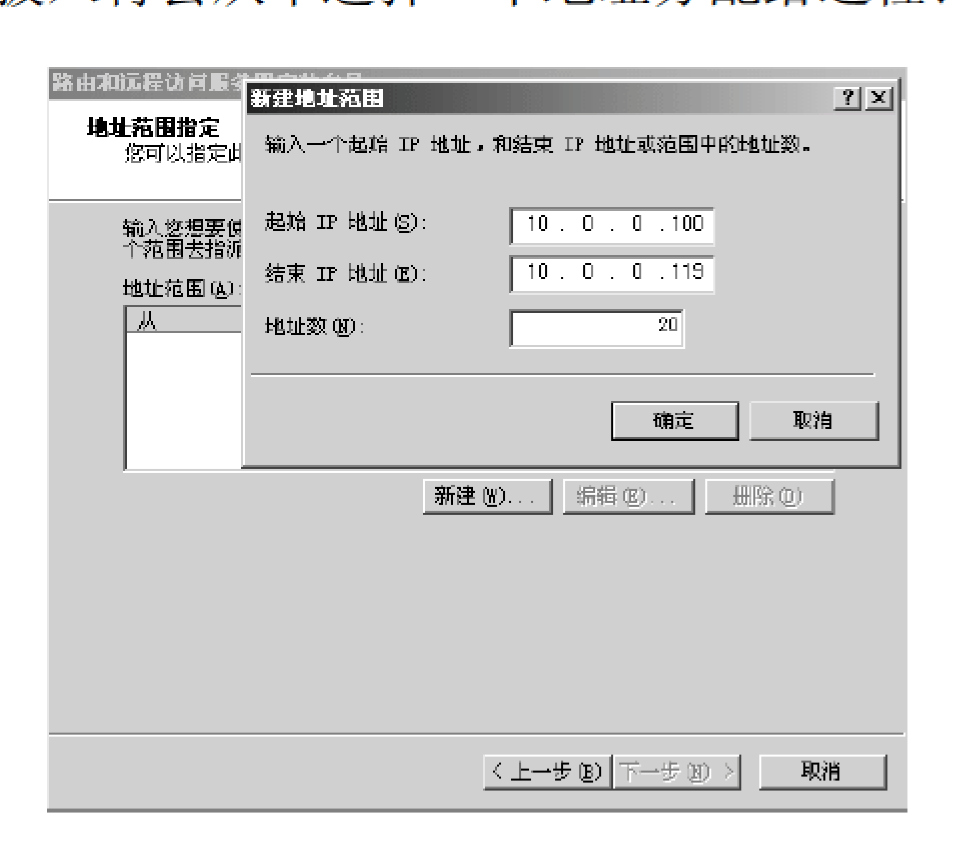
（7）如图 11-54 所示，在出现的“IP 地址指定”设置界面中，选中“来自一个指定的地址范围”，单击“下一步”按钮。



▲图 11-54　选择分配地址的方式

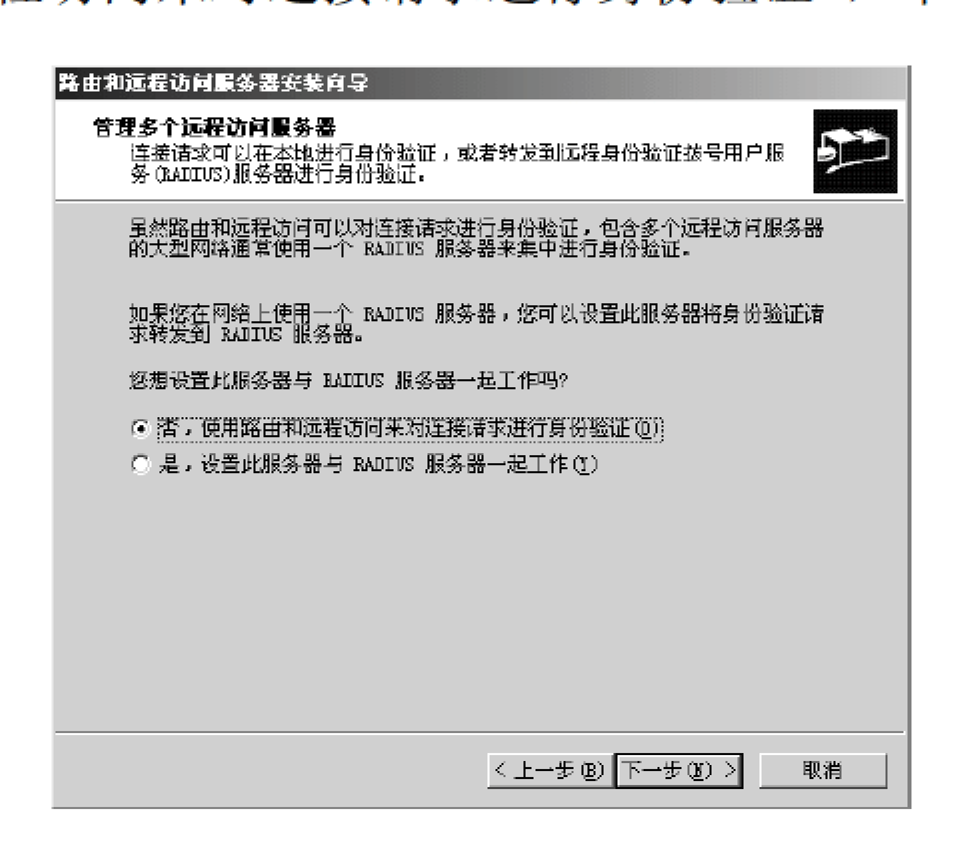
（8）如图 11-55 所示，在出现的“地址范围指定”设置界面中，单击“新建”按钮。

（9）如图 11-55 所示，在出现的“新建地址范围”对话框中，输入一个地址范围。远程计算机 VPN 拨入将会从中选择一个地址分配给远程计算机。



▲图 11-55　指定地址范围

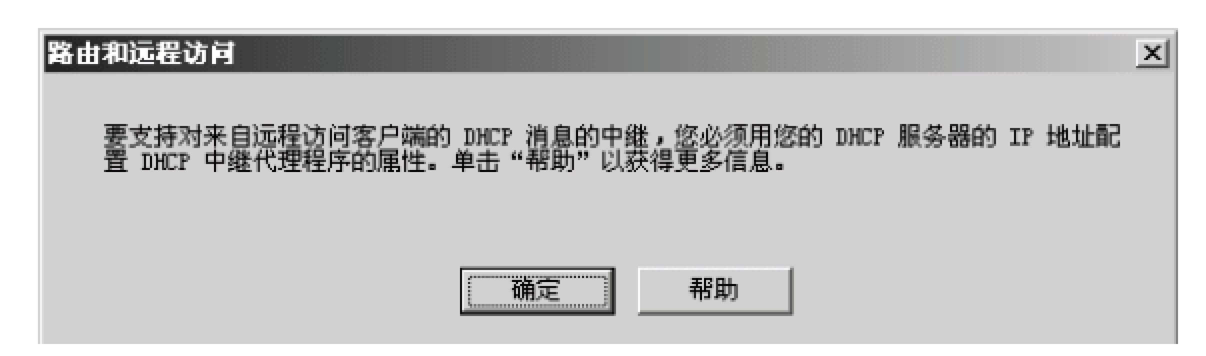
（10）如图 11-56 所示，在出现的“管理多个远程访问服务器”设置界面中，选中“否，使用路由和远程访问来对连接请求进行身份验证”，单击“下一步”按钮。



▲图 11-56　选择身份验证方式

（11）在出现的“完成路由和远程访问服务器安装向导”界面中，单击“完成”按钮，

（12）如图 11-57 所示，在出现的“路由和远程访问”提示对话框中，单击“确定”按钮。



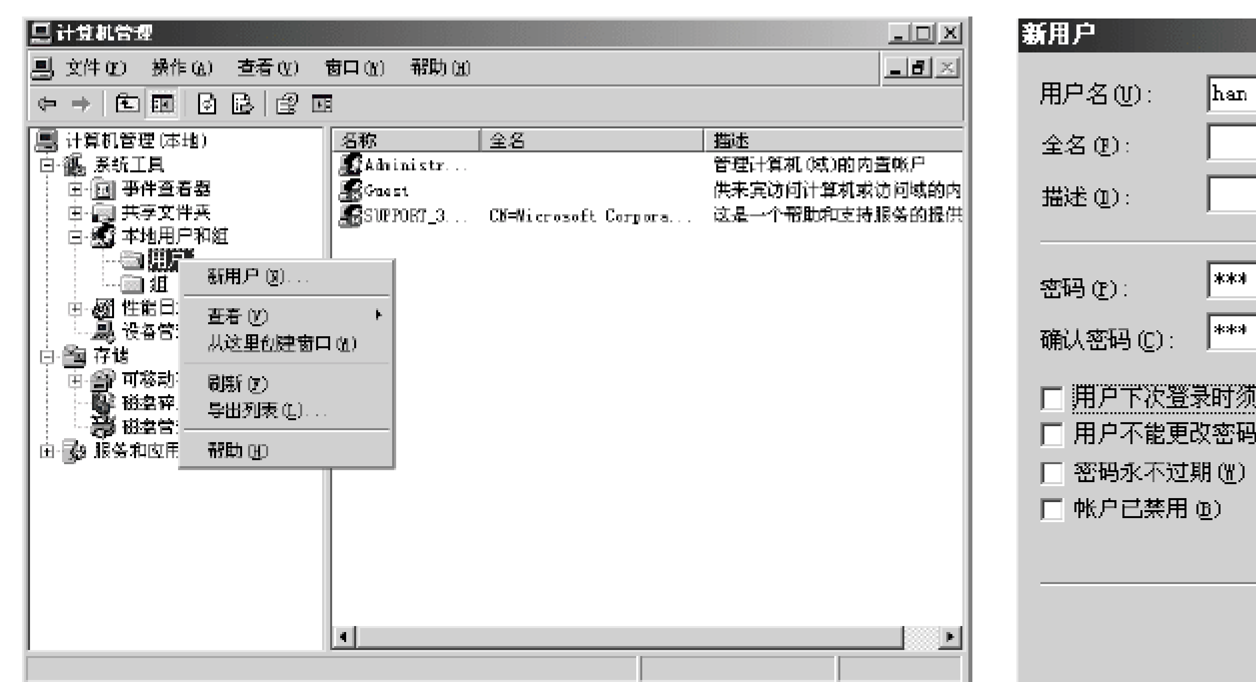
▲图 11-57　提示配置 DHCP 中继代理

2. 创建用户允许远程拨入

（1）选择“开始”→“程序”→“管理工具”→“计算机管理”命令。

（2）如图 11-58 所示，右击“用户”节点，在弹出的快捷菜单中选择“新用户”命令。

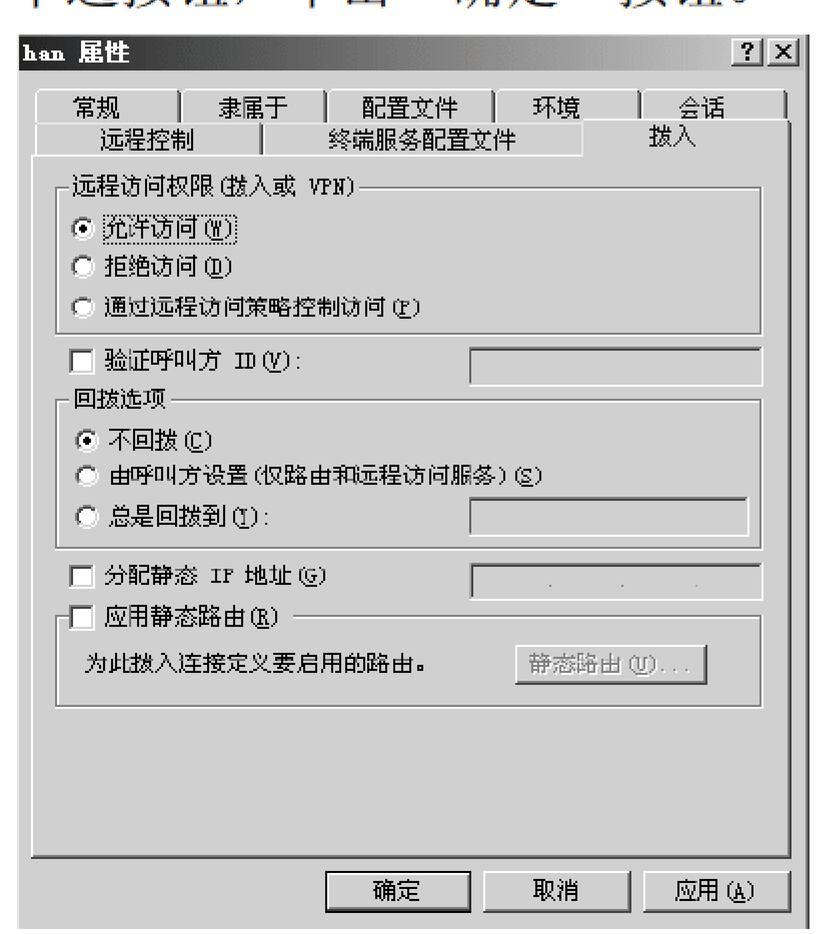
（3）如图 11-59 所示，在出现的“新用户”对话框中，输入用户名和密码，单击“创建”按钮。





▲图 11-58　选择“新用户”命令　　▲图 11-59　“新用户“对话框

（4）双击新用户，如图 11-60 所示，在出现的用户属性对话框的“拨入”选项卡中，选中“允许访问”单选按钮，单击“确定”按钮。



▲图 11-60　更改用户属性允许访问

远程访问服务器配置完毕。

下面介绍 RemotePC 如何建立 VPN 拨号连接访问 RAS。

3．建立 VPN 拨号

（1）在 RemotePC 上，选择“开始”→“设置”→“网络连接”命令。确保其能够和 RAS 连接 Internet 的网卡通信。

（2）如图 11-61 所示，在“网络连接”窗口中，单击“创建一个新的连接”命令。

（3）在出现的“欢迎使用新建连接向导”设置界面中，单击“下一步”按钮。

（4）在出现的“网络连接类型”设置界面中，选中“连接到我的工作场所的网络” 单选按钮，单击“下一步”按钮。

（5）在出现的“网络连接”设置界面中，选中“虚拟专用网络连接”单选按钮，单击

“下一步”按钮。

（6）在出现的“连接名”设置界面中，输入公司名称，单击“下一步”按钮。

（7）如图 11-62 所示，在出现的“VPN 服务器选择”设置界面中，输入 RAS 的公网地址，单击“下一步”按钮。

（8）在出现的“正在完成新建连接向导”设置界面中，选中“在我的桌面上添加一个到此连接的快捷方式”复选框，单击“完成”按钮。

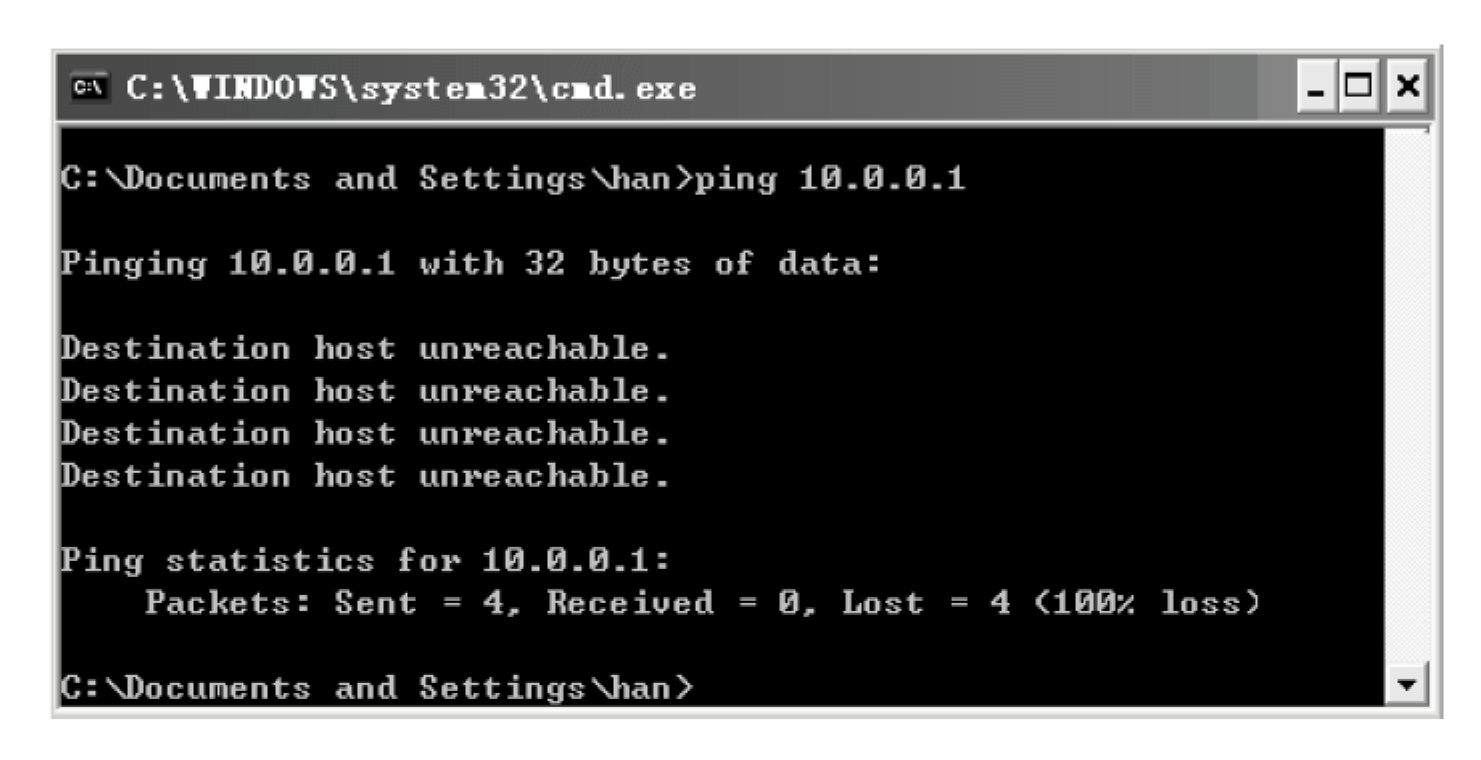


▲图 11-61 “网络连接”窗口



▲图 11-62 输入 RAS 的公网地址

（9）如图 11-63 所示，在 VPN 拨号之前，ping RAS 服务器的内网地址，不通。



▲图 11-63 测试到内网的连接

（10）如图 11-64 所示，双击刚才建立的 VPN 拨号连接，可以看到默认使用 PPTP 协议进行连接。输入用户名和密码，单击“连接”按钮。



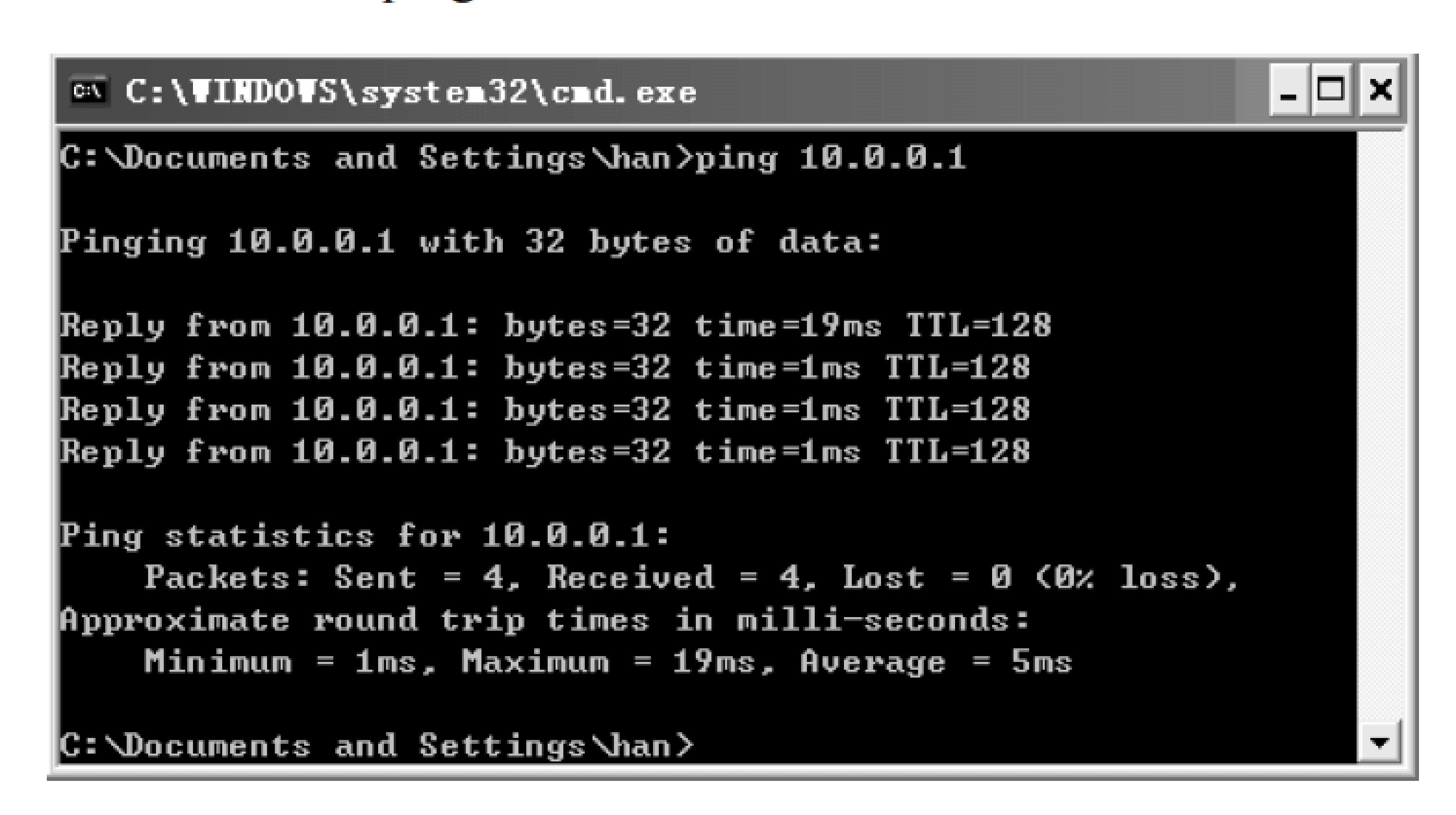
▲图 11-64 拨号连接

（11）如图 11-65 所示，拨通之后，在命令提示符下输入 ipconfig，可以看到 RAS 分配给该计算机的内网地址。



▲图 11-65　查看 VPN 建立的会话和 VPN 建立的连接

（12）如图 11-66 所示， ping RAS 的内网 IP 地址 10.0.0.1，可以看到能够 ping 通。



▲图 11-66　测试到内网的连通性

4．配置 VPN 使用 L2TP 协议

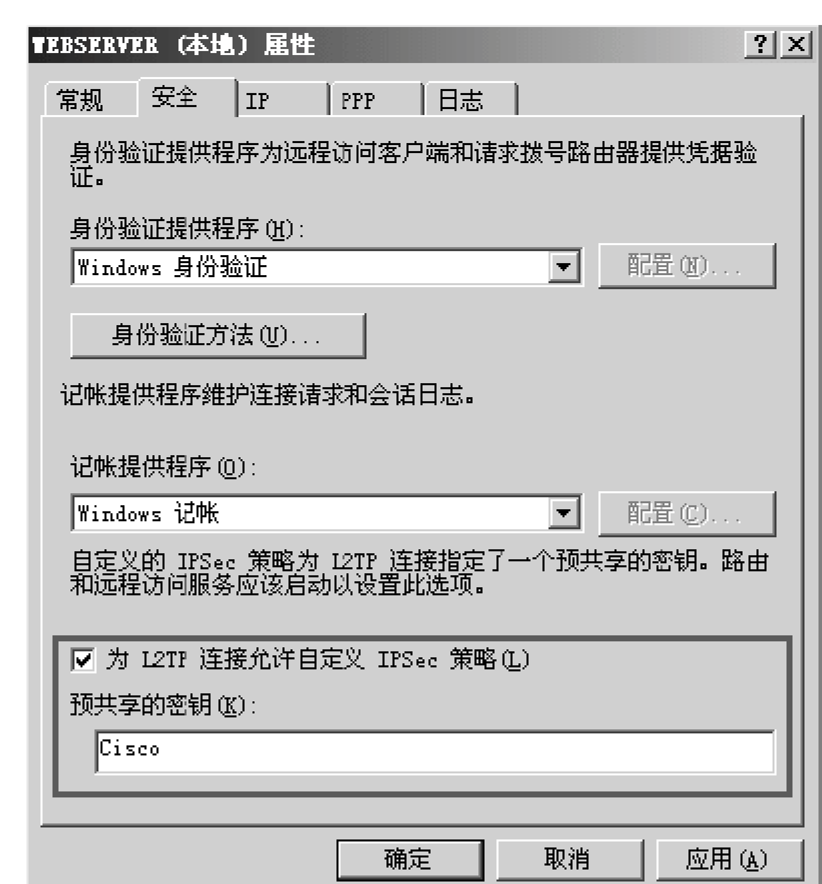
VPN 拨号默认使用的是 PPTP 协议，如果使用 L2TP 协议，则需要在远程访问服务器和客户端指定 IPSec 用来身份验证的共享密钥。

（1）如图 11-67 所示，在 RAS 上，打开“路由和远程访问”窗口，右击服务器，在弹出的快捷菜单中选择“属性”命令。

（2）如图 11-68 所示，在出现的服务器属性对话框的“安全”选项卡中，选中“为 L2TP 连接允许自定义 IPSec 策略”复选框，输入预共享的密钥，单击“确定”按钮。



▲图 11-67 选择“属性”命令



▲图 11-68 设置共享密钥

（3）如图 11-69 所示，在 RemotePC 上，右击建立的 VPN 连接，在弹出的快捷菜单中选择“属性”命令。

（4）如图 11-70 所示，在出现的连接属性对话框的“安全”选项卡中，单击“IPSec 设置”按钮。

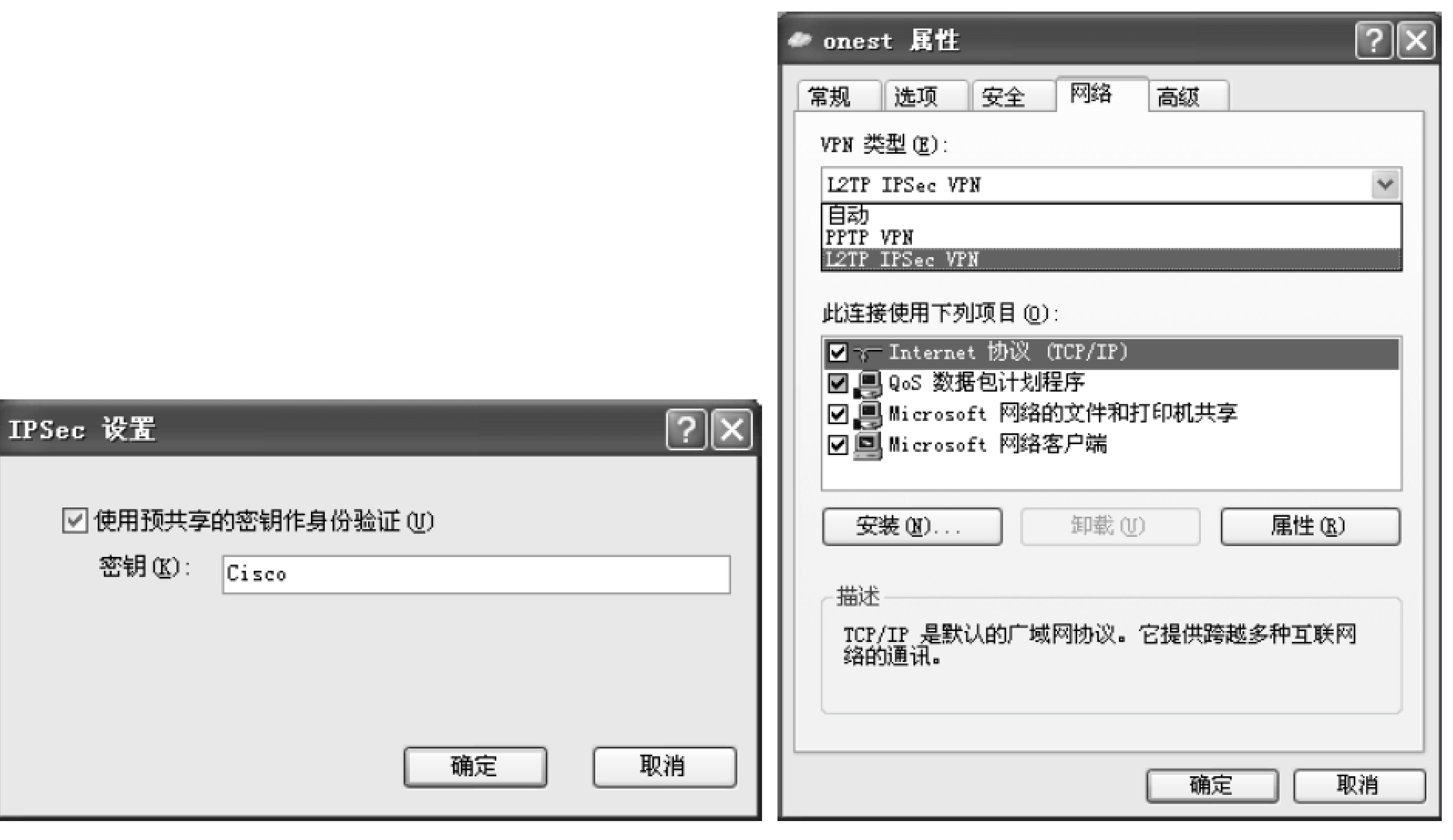


▲图 11-69 更改拨号连接属性

▲图 11-70 设置 IPSec

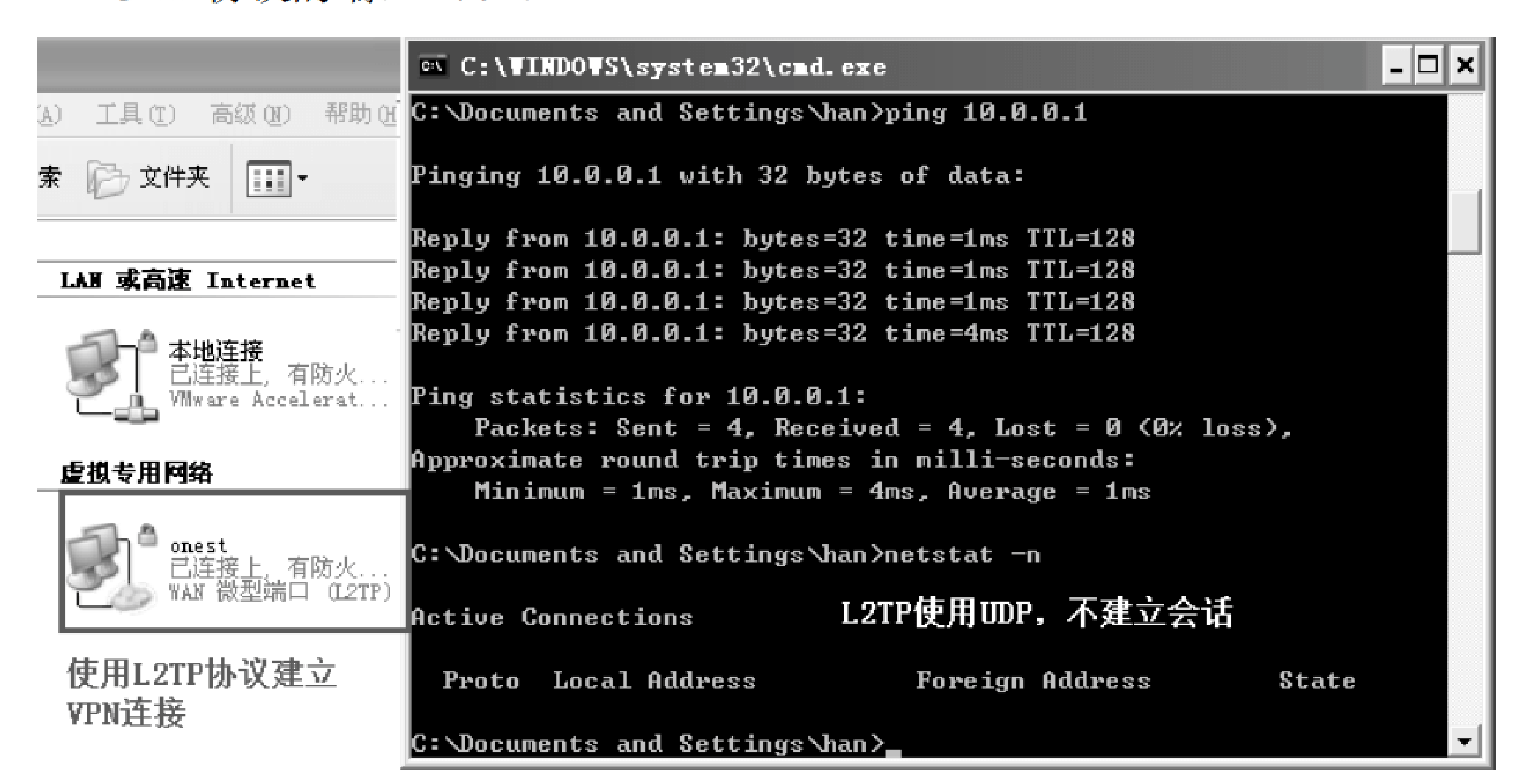
（5）如图 11-71 所示，在出现的“IPSec 设置”对话框，选中“使用预共享的密钥作为身份验证”复选框，输入密钥，单击“确定”按钮，这个密钥必须和 RAS 上指定的密钥相同。

（6）如图 11-72 所示，在属性对话框的“网络”选项卡中的“VPN 类型”下拉列表框中选中“LZTP IPSec VPN”选项，单击“确定”按钮。



▲图 11-71　设置 IPSec 共享密钥　　　　▲图 11-72　指定 VPN 类型

（7）如图 11-73 所示，连接，可以看到使用 L2TP 建立的 VPN 连接，能够 ping 通 RAS 内网的 IP 地址，输入 netstat –n 命令，看不到建立的会话。因为 L2TP 使用的是 UDP 协议的端口 1701。



▲图 11-73　使用 L2TP 拨通远程访问服务器

11.4 习 题

1. ________是广域网链路通常的封装。（选择所有正确答案）

A. Ethernet

B. PPP

C. Token Ring

D. HDLC

E. Frame Relay

F. POTS

2. 关于 PPP 特征的描述，下列_________是正确的描述。（选择所有正确答案）

A. 可封装多种不同的路由协议

B. 只支持 IP

C. 能够在模拟电路上应用

D. Cisco 专用

E. 支持错误诊断

3. 你准备将两个路由器的两个串口创建一个点到点的广域网连接，一端是 Cisco 路由器，另一端是华为路由器，应该使用________命令。

A. TK1（config-if）# encapsulation hdlc ansi

B. TK1（config-if）# encapsulation ppp

C. TK1（config-if）# encapsulation LAPD

D. TK1（config-if）# encapsulation frame-relay ietf

E. TK1（config）#encapsulation ppp

4. 关于描述帧中继点到点子接口的描述，下列_________描述是正确的。（选择两个答案）

A. 需要用来实现逆向 ARP

B. 每一个 DLCI 映射到一个单独的 IP 子网

C. 多个 DLCI 映射单一 IP 子网

D. 解决 NBMA（none broadcast multiaccess）水平分割

E. Requires use of the frame-relay map command

5. 你的帧中继网络在永久虚电路上使用 DLCI 信息，其目的是__________。

A. 它确定了帧中继的封装类型

B. 它们标识在本地路由器和帧中继交换机之间的逻辑虚电路

C. 它们代表路由器的物理地址

D. 它们代表永久虚电路的活跃

6. 下面_______命令能够应用到广域网接口，但是不能应用到局域网接口。（选择所有正确答案）

A. IP address

B. encapsulation PPP

C. no shutdown

D. PPP authentication CHAP

E. Speed

F. None of the above

7. 你正在配置的 Cisco 路由器接口使用 PPP 封装，支持________身份验证。（选择两个答案）

   A. SSL

   B. SLIP

   C. PAP

   D. LAPB

   E. CHAP

   F. VNP

8. 在一个实验中，两个路由器使用广域网接口连接，没有 DCE 设备，使链路 up，需要附加的命令。

   A. serial up

   B. clockrate

   C. clock rate

   D. dce rate

   E. dte rate

习题答案

1．B、 D、 E

2．A、C、E

3．B

4．B、D

5．B

6．B、D

7．C、E

8．C